Data Protection Policy

Date of Creation	November 2000
Date of Last Update	February 2025
Next Update Due	February 2026
Author	MIS
Responsible Manager	Director Of MIS And Funding
Approved by	The Governing Board
Date of Approval	16th December 2021
Date of Equality Impact Assessment	November 2000 (updated 2025)

Policy Statement

This policy sets out the guidelines in respect of the College's handling of data and its requirement to work under the auspices of the UK General Data Protection Regulation.

Background

The UK data protection legal framework is set out in the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. The Data Protection Act 2018 supplements the UK GDPR and provides additional provisions, particularly regarding areas not covered by the GDPR, such as law enforcement processing

The advancements in digital technology and the use of the internet have changed the way data is collected and processed. The UK GDPR provides for more safeguards of personal data and higher fines for noncompliance.

The UK GDPR relates not only to personal data processed by an automated system but also to manual filling systems where personal information is accessible based on specific criteria. This includes chronologically ordered manual filling systems. This may include personnel records or student registers or files which are indexed or any information collected with the intention that it will be filed in such a system. Data can be written information, photographs, or information such as fingerprints or voice recordings.

The UK GDPR applies to 'personal information'. The UK GDPR makes a distinction between personal data and 'special category' data (formerly 'sensitive personal data').

Personal information is defined as data relating to a living individual who can be identified d or indirectly from that information. It includes names and addresses, identification number, location data, online identifier, features such as hair and eye colour which may be in the form of photographs, ethnic origin, qualifications and experience, details about sick leave and holidays taken, birthdays and marital status. Any opinion about, or intentions regarding, a person that are recorded will also be personal information.

Special category data is defined as personal data consisting of information as to:

- Race
- Ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Criminal proceedings or convictions
- Health data
- Genetic and Biometric data where used for ID purposes

Introduction

The College must retain certain information about employees, students, and users to monitor performance, achievements, and health and safety. This data is also essential for recruiting and paying staff, organising courses, and meeting legal obligations to funding bodies and the government. To comply with the law, information must be collected and used fairly, stored securely, and not disclosed unlawfully, in accordance with the UK General Data Protection Regulation.

Personal data must be:

1. Processed lawfully, fairly, and transparently in relation to individuals.
2. Collected for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes. Further processing for archiving in the public interest, scientific, historical, or statistical purposes is permitted under Article 89(1) of the UK GDPR.
3. Adequate, relevant, and limited to what is necessary for the purposes of processing.
4. Accurate and kept up to date; reasonable steps must be taken to rectify or erase inaccurate data without delay.
5. Stored in a form that allows identification of data subjects for no longer than necessary; longer storage is allowed for archiving purposes, provided appropriate safeguards are in place.
6. Processed securely, protecting against unauthorised access, loss, destruction, or damage through appropriate measures.
7. Accountable, with the responsibility to demonstrate compliance with these principles.

Personal information may only be transferred overseas to countries that have an adequate level of protection of personal data.

The College and its staff must always adhere to data protection principles. To ensure compliance, the College has established this Data Protection Policy.

Additionally, the College conducts Data Protection Impact Assessments (DPIAs) as mandated by the UK GDPR, integrating them into procurement processes and other relevant areas.

Status of the Policy

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 who considers that the policy has not been followed in respect of personal information 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.

Notification of Data Held and Processed

All staff, students, and other users are entitled to know the following regarding their personal information held by the College:

- What Information is Held: Users have the right to understand what personal data the College processes about them, including details such as academic records, contact information, and any other relevant data. This information is used for purposes such as academic support, communication, and compliance with legal obligations.

- How to Gain Access: Users can request access to their personal data by submitting a formal request to the College's Data Protection Officer (DPO). The College is committed to responding to such requests promptly and within the timeframe specified by the UK GDPR.

- How to Keep Information Up to Date: It is essential for users to keep their personal information accurate and current. The College provides guidance on how to update personal details, typically through online portals or by contacting relevant administrative offices.

- Compliance with UK GDPR: The College is dedicated to fulfilling its obligations under the UK GDPR. This includes implementing appropriate security measures, conducting regular training for staff, and ensuring transparency in data processing activities.

The College will provide, upon request, staff, students, and other relevant users with access to their personal information held in its systems, in accordance with the UK GDPR and the individual's right of access. This process ensures that users can verify the accuracy of their data and understand how it is being used.

If you would like to exercise any of these rights, please contact the Data Protection Officer at dataservices@judicium.com

Responsibilities of Staff

All staff are responsible for:

- Ensuring Accuracy: Checking that any information they provide to the College regarding their employment is accurate and up to date.
- Reporting Changes: Informing the College of any changes to the information they have provided, such as a change of address.
- Reviewing Information: Regularly checking the information the College sends out, which details the data held and processed about them.
- Notifying Errors: Informing the College of any errors or changes. The College cannot be held responsible for inaccuracies unless the staff member has notified the College in writing.

Additionally, when staff collect information about others (e.g., students' coursework, assessments of abilities, references to other educational institutions, or details of personal circumstances), they must adhere to the guidelines outlined in Appendix 1.

Data Security

All staff are responsible for ensuring that:

- Security of Personal Information: Any personal information they hold is kept secure and protected from unauthorised access.
- Confidentiality: Personal information is not disclosed, whether orally, in writing, electronically, or accidentally, to any unauthorised third party.

Staff should be aware that unauthorised disclosure of personal information is a serious matter and may lead to disciplinary action, including potential gross misconduct.

Personal information should be stored securely by:

- Keeping it in a locked filing cabinet.
- Storing it in a locked drawer.
- Ensuring that computerised data is password protected.

Additionally, staff must complete the required training on Data Protection and stay updated with the College's information security guidelines to ensure compliance and safeguard personal data.

Student Obligations

Students must ensure that all personal information provided to the College is accurate and up to date. They must ensure that changes of address etc. are notified to their personal tutor or Learner Services.

Students who utilise the College's computer facilities may occasionally process personal data as part of their coursework or projects. It is crucial for students to understand their responsibilities in handling this data to ensure compliance with data protection regulations.

Rights to Access Information

Staff, students and other users of the College have the right to access any personal information that is being kept about them either in a computer system or a manual filling system. Any person wishing to exercise this right may do so by contacting the Data Protection Officer at dataservices@judicium.com. The data subject making such a request will be required to produce proof of their identity.

The College reserves the right to refuse a personal information request or to charge a reasonable fee for administrative costs if it deems the request unfounded or excessive. If a request is denied, the College will provide the individual with the reason and inform them of their right to complain to the Information Commissioner's Office (ICO).

The College aims to respond to requests for access to personal information promptly, typically within one month. If there are valid reasons for a delay, such as multiple or complex requests, the College will communicate the reasons in writing within one month of receiving the request.

For further assistance, individuals can contact the ICO at:

Helpline: 0303 123 1113
Website: ico.org.uk

Publication of College Information

It is College policy to make certain information public such as:

- Names of the College Corporation Members and Register of Interests of those members.
- Non confidential minutes and papers of full Corporation meetings.

Processing Special Category Data and Criminal Convictions

Sometimes, it is necessary for the College to process sensitive information about individuals, including their health, race, gender, family details, and criminal convictions. This processing is essential for several reasons:

1. Safety and Well-being: Understanding health conditions can help the College provide appropriate support and accommodations, ensuring a safe and inclusive environment for all students and staff. For instance, this may involve implementing measures for individuals with disabilities or health issues.

2. Compliance with Legal Obligations: The College must adhere to various legal requirements, such as safeguarding laws and health and safety regulations. Processing information about criminal convictions may be necessary for roles that involve working with vulnerable populations, ensuring that the College maintains a safe environment.

3. Equalities Policy: The College is committed to promoting equality and diversity. By processing data related to race and gender, the College can monitor its compliance with the Equalities Policy, identify any disparities, and implement strategies to promote inclusivity and equal opportunities for all.

4. Support Services: Information about family circumstances may be relevant for providing tailored support services, such as counselling or financial aid.

5. Data Protection Compliance: The College ensures that all processing of sensitive information is conducted in accordance with the UK GDPR, with appropriate safeguards in place to protect individuals' privacy and rights.

By processing this information responsibly, the College aims to foster a supportive and secure educational environment for everyone.

Examination Marks

Students are entitled to receive information about their marks for both coursework and examinations. They can also request access to their marked exam papers; however, the Exam Board may charge a fee for this service.

Retention of Data

The College recognises that the efficient management of its records is essential to support its core functions and comply with legal and regulatory obligations. Proper data retention practices ensure that the College can:

- Support Academic and Administrative Functions: Retaining records allows the College to track student progress, manage course offerings, and facilitate effective communication with students and staff.

- Comply with Legal Requirements: The College adheres to various laws and regulations that dictate how long certain types of data must be retained, such as student records, financial documents, and employment information.

- Protect Individual Rights: By maintaining accurate records, the College can uphold the rights of students and staff, ensuring that they have access to their information and can verify its accuracy.

- Implement Data Minimisation: The College is committed to retaining data only for as long as necessary, ensuring that outdated or irrelevant information is securely disposed of in accordance with data protection regulations.

The College regularly reviews its data retention policies to ensure compliance and to adapt to changing legal requirements and best practices in data management.

Conclusion

Compliance with the UK General Data Protection Regulation (UK GDPR) is the responsibility of all members of the College. Any deliberate breach of the data protection policy will lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Data Protection Officer.

Data Protection Officer

The Data Protection Officer is responsible for overseeing data protection within the College. Should you have any questions, concerns or queries please contact them on the following information:

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 (Option 1, then 1)

APPENDIX 1

Staff Guidelines for Data Protection

College staff regularly process student information for tasks such as marking registers, grading coursework, writing reports, or providing pastoral or academic supervision. The College ensures that all students are informed about the categories of data processing through registration procedures and privacy notices, as required by the UK GDPR. The day-to-day information handled by staff typically includes:

- General personal details (e.g., name and address)
- Class attendance, coursework marks, and grades
- Notes on personal supervision, including behaviour and discipline matters.

Sensitive information, such as a student's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity, or race, is often restricted to staff who need to know.

Compliance with UK GDPR Principles

All staff must comply with the UK GDPR principles outlined in the College's Data Protection Policy. Specifically, records must be:

- Accurate
- Up to date
- Fair
- Kept and disposed of safely, in accordance with College policy.

Authorised Staff

The College designates certain staff as 'authorised staff', who are permitted to handle or process non-standard or Special Category Data. Exceptions are allowed if a non-authorised staff member deems the processing necessary and:

- It is in the best interests of the student, staff member, third party, or the College, and
- The authorised person has been informed, or the processing is urgent and necessary under the circumstances.

These exceptions should be rare.

Security and Disclosure

Authorised staff are responsible for ensuring that all information is kept secure. Staff must not disclose personal information to any student, except for normal academic or pastoral purposes, without proper authorisation or in line with College policy. Similarly, personal information should not be disclosed to other staff members without authorisation or in line with College policy.

Staff Checklist for Recording Information

Before processing any personal information, staff should consider the following checklist:

- Do you really need to record the information?
- Is the information 'standard' or 'sensitive'?
- If sensitive, record why and any special handling conditions.

- Has the student been informed that this type of information will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the individual that the data is accurate?
- Are you sure that the information is secure?
- Are you satisfied that it is in the best interests of the student or staff member to collect and retain the information?
- Have you reported the information collection to the authorised person within the required time?
- Have you ensured that only the minimum necessary data is collected?
- Have you scheduled regular reviews to ensure the data remains accurate and relevant?
- Are there specific security measures in place to protect the data (e.g., encryption, access controls)?
- Have you read and understood the Data Access Policy?

APPENDIX 2

How to Report a Data Breach

A data breach occurs when unauthorised individuals gain access to sensitive, confidential, or protected information. This can happen through various means, such as hacking, phishing, malware, or even accidental exposure. The compromised data can include personal information, financial records, intellectual property, or any other type of sensitive data.

Data breaches can have serious consequences, including identity theft, financial loss, and damage to the College's reputation. It's important for individuals to take steps to protect their data, such as using strong passwords, enabling two-factor authentication, minimising the use of Excel spreadsheets and data silos, and ensuring that security updates have been applied to all systems.

In the event of an actual or suspected data breach:

1. **If you suspect you have caused a data breach** and the breach has occurred by email, immediately attempt to recall the message. If data has been accidentally sent to external recipients, email recall is unlikely to work.

    a. If email recall is not possible, consider sending an immediate follow-up message to the recipients advising that data has been sent in error, and asking recipients to delete the data.

2. **If you suspect you have caused a data breach or you have information pertinent to a breach**, immediately report the incident to your line manager and the Director of MIS and Funding. The Director of MIS and Funding acts as the Data Protection Officer's authority within the College and will be able to provide guidance.

3. If you are unable to provide an immediate report to your line manager and the Director of MIS and Funding provide a short summary of the incident by email to the Data Protection Officer, Judicium, dataservices@judicium.com and also to the Executive Office, executive.office@barnetsouthgate.ac.uk

    Note that in all instances **any member of ELT** is also a valid route to ensure prompt attention to a data breach. The critical objective is to communicate and respond to the need arising.

4. Make a note of the timings of the incident, the scope and impact of the data shared, and your follow up actions which will be needed if the incident is deemed reportable to the Information Commissioner's Office (ICO).

5. Ensure you have completed relevant mandatory training, including Data Protection and Cyber Security.

Following a data breach report it may be decided that further containment actions, communications, security measures and/or training are deemed necessary.

APPENDIX 3

Data Protection Impact Assessment (DPIA)

1. Introduction

This DPIA is conducted to ensure that the data processing activities within the College comply with the UK GDPR and other relevant data protection legislation. The aim is to identify and mitigate any potential risks to the rights and freedoms of individuals whose data is processed by the College.

2. Purpose

The purpose of this DPIA is to:

- Assess the necessity and proportionality of data processing activities.
- Identify and evaluate potential data protection risks.
- Implement measures to mitigate identified risks.
- Ensure compliance with data protection principles and enhance accountability.

3. Scope

This DPIA covers all personal data processing activities related to the College's Data Protection Policy, including but not limited to:

- Student records
- Staff records
- Academic and pastoral supervision records
- Administrative records

4. Description of Processing

Nature of Processing:

- Collection, storage, use, and sharing of personal data for academic, administrative, and pastoral purposes.

Types of Data:

- Standard data: Name, address, attendance, grades, etc.
- Special Category Data: Health information, ethnicity, religious beliefs, etc.

Data Subjects:

- Students
- Staff
- External stakeholders (where applicable)

Processing Activities:

- Application and enrolment
- Academic assessments
- Pastoral care
- Administrative functions

5. Necessity and Proportionality

The processing of personal data is necessary for the College to fulfil its educational and administrative functions. The data collected is proportionate to the purposes for which it is processed, ensuring that only the minimum necessary data is collected and processed.

6. Consultation Process

Stakeholders consulted during this DPIA include:

- Data Protection Officer (DPO)
- MIS Department
- Technology and Innovation Department
- Campus Directors

7. Risk Assessment

Identified Risks:

- Unauthorised access to personal data
- Data breaches
- Inaccurate data processing
- Non-compliance with data protection principles

Risk Evaluation:

- Likelihood: Medium
- Impact: High

8. Mitigation Measures

Technical Measures:

- Encryption of sensitive data
- Access controls and authentication mechanisms
- Regular security audits

Organisational Measures:

- Staff training on data protection
- Clear data protection policies and procedures
- Regular reviews and updates of data protection practices

9. Documentation and Review

The results of this DPIA will be documented and reviewed regularly to ensure ongoing compliance with data protection legislation. Any changes to data processing activities will trigger a review of this DPIA.

10. Conclusion

This DPIA has identified potential risks associated with the College's data processing activities and outlined measures to mitigate these risks. By implementing these measures, the College aims to ensure the protection of personal data and compliance with the UK GDPR.