

## **Queen Mary's College – Privacy Notice**

Queen Mary's College (QMC) is an Academy within the North Hampshire Education Alliance (NHEA) Multi-Academy Trust. The College, on behalf of the NHEA, is the Data Controller of the personal data that it collects and receives.

The College has one Data Protection Officer (DPO) – Toni Baldwin, Academy Secretary, and two Data Protection Liaison Officers - Sally-Anne Spooner (Director of Human Resources and Commercial Operations) and Caroline Watson (Director of College Support). The following email address can be used by anyone external to the organisation wishing to make contact – [info@qmc.ac.uk](mailto:info@qmc.ac.uk)

The College is registered as a Data Controller under the Data Protection Act 2018. Our registration number is Z6760455. The College is considered a public authority.

### **Purpose**

This notice sets out how the College deals with personal data correctly and securely and in accordance with the GDPR, and other related legislation. The notice applies to all personal data however it is collected, used, recorded and stored by the College and whether it is held on paper or electronically.

QMC collects and uses personal data about staff, students, parents, customers and other individuals who come into contact with the College. This information is gathered in order to enable the provision of education and other associated functions. The College will ensure that the legal basis for processing data will be complied with. For further information please see Appendix A.

The College issues a Privacy Notice to students when they apply online and when they sign the learner agreement. The privacy notice summarises the personal data held, the purpose for which it is held and with whom it may be shared. It also provides information about an individual's rights in respect of their personal data.

### **Why we collect and use personal data**

We collect and use personal data:

- To administer the application process
- To support student learning
- To monitor and report on student progress
- To provide appropriate pastoral care
- To assess the quality of our services and how well College is performing
- For statistical forecasting and planning
- To comply with the law regarding data sharing

### **Types of personal data we collect, hold and share**

- Personal data (such as: name, address, DOB, unique pupil number, parent/guardian contact information, photographic ID)
- Characteristics (such as: ethnicity, language, nationality, country of birth and free school meal eligibility, bursary, disability)
- Attendance information (such as: classes attended, number of absences and reason) and exclusion data
- Assessment information (such as: in-class progress, UCAS, career aims, exam results)
- Modes of travel
- Relevant medical, special educational needs and behavioural information

### **Why we collect and use personal data**

Learner data is collected by the College in order to administer student education and welfare in accordance with the terms and conditions of funding imposed on us as providers of learning. You must provide it in order to enrol at the College.

Whilst the majority of personal data you provide to us directly as part of the application process is mandatory, some of it is provided voluntarily and we will seek consent (such as: using a student's image in marketing materials, seeking permission from a parent/guardian for a student to leave site to attend off-site trips). Where we are using your personal data only on the basis of your permission you may ask us to stop processing this personal data at any time.

Sensitive personal data you provide (eg. disability or ethnicity) may be used by the College for the purposes of equality of opportunity, support for your studies and to minimise risk. It may also be used anonymously for statistical purposes. The College will ask your permission before sharing sensitive information with other organisations, unless the sharing is permitted by law and necessary.

You may be contacted after you have completed your programme of learning to establish whether you have entered employment or gone onto further training or education. This is called destinations information and this may be shared as detailed below should you choose to provide it.

### **The legal basis for collecting personal data - general**

The College passes most of the data it collects to Government agencies to meet funding arrangements. The College is a Data Processor for the Education and Skills Funding Agency (ESFA). Data may also be shared with the Department for Education (DfE), the Local Authority (LA) and the Sixth Form Colleges Association (SFCA). Information is used for the exercise of functions of these government departments and organisations to meet statutory responsibilities. It is also used to create and maintain unique learner numbers (ULNs) and Personal Learning Records (PLRs).

The data provided may be shared with other organisations for the purposes relating to education, training, employment, career and general advice services, well-being (eg, the Safeguarding Partnership or other partnerships as required), statistical and research purposes. Data sharing underpins college funding, educational attainment and monitoring. We do not share your information for purposes that are incompatible, such as product marketing. Data sharing will only take place where the sharing is in compliance with the law.

When personal data is Special Category information (such as: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics for ID purposes, health, sexual orientation) we may rely on processing being in the substantial public interest in addition to the vital interest of the data subject or another. Data is used for the purpose of monitoring equality of opportunity or treatment between different groups. Safeguards are in place to ensure data is held securely in accordance with our retention policy.

Our requirement for personal data and our legal basis for processing data includes the Education Act 1996, 2002 and 2011, the Children's Act 1989, the Equalities Act 2010, the Academies Act 2010 and Companies Act 2006.

### **The legal basis for collecting personal data - specific to:**

- **16 and 17 year olds**
- **Vulnerable 18 year olds ('vulnerable' is defined locally by individual Local Authorities)**
- **18-25 year olds with an Education Health Care Plan (EHCP)**

The Education and Skills Act 2008 (the Act) places duties on local authorities (LAs) to promote the effective participation in education or training of all 16 and 17 year olds resident in their area, and to make

arrangements to identify young people resident in their area who are not participating. It is part of the LA's duties to secure sufficient suitable education and training provision for all 16-19 year olds, and to encourage, enable and assist young people to participate in learning.

Under the Act, it is the College's duty to provide relevant information about their students to the LA of each student's residence, when requested to do so, and notify local LAs when a young person leaves learning at the College. All educational institutions are required to share information with LAs as part of their duty under the Act. Section 72 of the Act provides the legal basis for sharing information between LAs and educational institutions so that they are able to report monthly to the Department of Education and deliver their duties.

### **Personal data and parents/guardians/carers details**

Under data protection, young people aged 16 and over can decide for themselves and give consent for the processing of their personal data. Parental consent is not required. There may be exceptions in regards of students with severe learning difficulties and those who are otherwise unable to decide for themselves.

The College has found that it is very beneficial to the young person's progress as a student if the College is able to engage with the parents (or guardian/carer). Therefore it is very important that we hold these details on our systems.

When a student is in Further Education, parents/carers/guardians (or any other third party) are not automatically entitled to the student's information. We can only release information about our students if we have their consent for this recorded on the College system. Students are asked for their consent for sharing information with parents/others by completing this information on the online enrolment form, or when enrolling face-to-face.

### **Storing personal data**

Data, personal and special category, is only accessed by staff trained to administer the processes associated with College/educational activities. We hold personal/special category data securely either on in-house servers or servers/cloud storage hosted within Europe. Data is held in accordance with our retention schedule; nominally this is seven years, but there may be categories of data for which different retention rules apply (eg: child protection files).

### **Websites and cookies**

During your visit to our website we do not record any personal data from you or your computer. All details such as your name and address that are required to complete online enquiries will be used solely for that purpose and will not be made available to anyone not involved in that process. We will never share your email address or any other personal details you have supplied with any third party.

A 'cookie' is a small text file that is stored on your computer or mobile device when you visit a website. They are used to help remember settings, information you have given and for measuring how you use the website so that we can make sure it meets your needs.

To learn more about cookies visit: [www.aboutcookies.org.uk](http://www.aboutcookies.org.uk)

We use Google Analytics to collect information about how people use our website. This information is used for analysis and to help improve usability of the sites. We do not track or record information about individuals and their visits. We may compile and report aggregate statistics about our users such as visitor numbers, and related site information; however, these statistics will not include personally identifying information.

### **Subject Access Rights (SARs)**

Under data protection legislation, data subjects have the right to request access to information held about them. To make a request for personal data, contact the Data Protection Officer at [info@gmc.ac.uk](mailto:info@gmc.ac.uk) and mark the enquiry 'data protection request'.

- The right of access – Individuals have the right to access their personal data. This will be provided as quickly as possible. We are legally bound to provide data within one calendar month. This data will usually be provided free of charge unless the request is considered unfounded, excessive or repetitive.
- The right to rectification – Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
- The right to erasure – An individual is entitled to request the deletion or removal of personal data where there is no compelling reason for its continued processing. It should be noted that the College is legally obliged to process and retain much of the personal information we hold.
- The right to restrict processing – Individuals have the right to restrict the College from processing certain aspects of their personal data if one of the following circumstances applies:
  - The accuracy of the data is contested
  - The College's processing of the data is unlawful
  - The College wishes to delete the data, but the individual has need of the data for legal purposes.
- The right to data portability – Individuals may request an electronic copy of their personal data to use for their own purposes. The college will make every effort to provide the data in a form that is useable and acceptable to the individual.
- The right to object – Individuals have the right to object to:
  - Direct marketing – the College will stop processing for this purpose on receipt of an objection. It is not common practice for the College to engage in this type of activity.
  - Data processing for research – the College will engage with the individual to come to an agreement within the law.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at [www.ico.gov.uk](http://www.ico.gov.uk)

### **Contact(s)**

Data Protection Officer (DPO) – Toni Baldwin, Academy Secretary, NHEA

Data Protection Liaison Officer - Director of Human Resources and Commercial Operations, QMC

Data Protection Liaison Officer - Director of College Support, QMC

The following email address can be used by anyone external to the organisation wishing to make contact – [info@gmc.ac.uk](mailto:info@gmc.ac.uk)

## APPENDIX A - LEGAL BASIS FOR PROCESSING

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- d) Vital interests: the processing is necessary to protect someone's life.
- e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If you are processing for purposes other than legal obligation, contract, vital interests or public task, then the appropriate lawful basis may not be so clear cut. In many cases you are likely to have a choice between using legitimate interests or consent. You need to give some thought to the wider context, including:

- Who does the processing benefit?
- Would individuals expect this processing to take place?
- What is your relationship with the individual?
- Are you in a position of power over them?
- What is the impact of the processing on the individual?
- Are they vulnerable?
- Are some of the individuals concerned likely to object?
- Are you able to stop the processing at any time on request?

You may prefer to consider legitimate interests as your lawful basis if you wish to keep control over the processing and take responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them. On the other hand, if you prefer to give individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed), you may want to consider relying on individuals' consent.

The lawful basis for your processing can also affect which rights are available to individuals. For example, some rights will not apply:

	<b>Right to erasure</b>	<b>Right to portability</b>	<b>Right to object</b>
Consent			<b>x</b> but right to withdraw consent
Contract			<b>x</b>
Legal obligation	<b>x</b>	<b>x</b>	<b>x</b>
Vital interests		<b>x</b>	<b>x</b>
Public task	<b>x</b>	<b>x</b>	
Legitimate interests		<b>x</b>	