Queen Mary's College - Data Protection Policy

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

The College is registered as a Data Controller under the Data Protection Act 1998 and, from 25 May 2018, under the General Data Protection Regulation (GDPR). Our registration number is Z6760455. The College is considered a public authority.

Purpose
This policy sets out how the College deals with personal data correctly and securely and in accordance with the GDPR, and other related legislation. The policy 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.

What is Personal Data?
Personal data means any information relating to a living, identified or identifiable individual. An identifiable individual is one who can be detected, directly or indirectly, by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's name, address, date of birth, photograph, bank details and other information that identifies them.

What is Sensitive Personal Data?
Also known as Special Category Data, this is the subset of personal data where the data items are especially sensitive and need a greater level of protection. These include: ethnic origin, health data, religion, sexual orientation and biometric information.

Data Protection Principles

It is an offence to process personal data except in strict accordance with the principles and duties of data protection.

- Personal data shall be processed fairly, lawfully and in a transparent manner.
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes).
- Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive.
- Personal data shall be accurate and where necessary, kept up to date.
- Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Personal data shall be processed in a manner that ensures appropriate security of the personal data.

Data Protection Duties
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures adequate levels of data protection.
- Data controllers have a general duty of accountability for personal data.

Responsibilities
The College has responsibility to collect and hold information in accordance with the Act. Ultimate responsibility for ensuring compliance with this policy lies with the NHEA. The Academy Secretary, Director of Human Resources and Director of College Support hold day to day responsibility for co-ordinating the Data Protection on behalf of the College.

Compliance with this policy is compulsory for all staff, casuals or anyone working on behalf of the College. A member of staff who fails to comply with the policy may be subject to disciplinary action under the College's disciplinary procedures. All staff will be made aware of the existence of the policy and its content through regular training.

Commitment
- The identity and contact details for the Data Controller and Data Protection Officer will be displayed on the website and College intranet.
- Individuals are notified of the basis and purpose of the collection of personal data through the College's Privacy Statement available on the website and online application system. How we use personal data also forms part of the enrolment form/learner agreement.
- Data will be kept no longer than it is required and destroyed appropriately and securely.
- Data will only be accessed by those authorised to process data.
- Clear and robust safeguards are in place to ensure personal data is kept securely from inappropriate use, loss, theft, unauthorised disclosure, irrespective of the format in which it is recorded.
- Data will only be shared with others when it is legally appropriate to do so.
- We recognise our duty to respond to requests for access to personal data (Subject Access Requests).

Subject Access Requests (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@qmc.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 – Individuals are 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

Loss or Theft of Personal Data

All incidences of loss or theft of personal data must be reported immediately to the College's Data Controller. In the case of a potential breach, the Data Controller will instigate an investigation into the incident and will decide whether it needs to be reported to the Information Commissioner's Office (ICO). If a breach has occurred, the ICO will be informed within 72 hours of the incident. If appropriate, the data subjects concerned will also be informed. The Data Controller will retain a central register of all such incidents occurring within the College.

Complaints

Complaints will be dealt with in accordance with the College's complaints policy. Complaints relating to the handling of personal data may be referred to the Information Commissioner who can be contacted at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years. The policy review will be undertaken by the Data Protection Officer, Data Protection Liaison Officers, Principal and nominated representative.

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@qmc.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:

	Right to erasure	**Right to portability**	**Right to object**
Consent			✘ but right to withdraw consent
Contract			✘
Legal obligation	✘	✘	✘
Vital interests		✘	✘
Public task	✘	✘	
Legitimate interests		✘	