Queen Mary's College - General Data Protection Policy

Queen Mary's Sixth Form College collects and uses personal information about applicants, students, parents, staff and other individuals who come into contact with the College. This information is gathered in order to enable the provision of education, monitor the performance and achievements of students and safeguard the health, safety and security of the College community, particularly in relation to our child protection responsibilities.

Other information relates to the College in its role as an employer so that staff can be recruited and paid. The College also has to meet its legal obligations to funding bodies and government agencies.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. As part of its working practices, The College must comply with the General Data Protection Regulation 2018 (GDPR).

The College has Privacy Notices detailing the purpose for which information is held and with whom it may be shared.

Data Controller

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. The College determines what personal information is collected and how it is processed and held.

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 (Assistant Principal, Organisational 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. Our registration number is Z6760455. The College is considered a public authority.

Purpose

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

Data Protection Principles

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner
2. 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)
3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive
4. Personal data shall be accurate and where necessary, kept up to date
5. 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;
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Consent

A Data Subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action. Data Subjects are able to withdraw consent to processing at any time and withdrawal must be actioned promptly. Consent may need to be refreshed if it is to be used for a different purpose which was not disclosed when the Data Subject first consented.

Explicit Consent is required for processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. The Privacy Notice identifying the Sensitive Personal Data and the purpose for collection must be available to the Data Subject.

Evidence of consent must be recorded so that the College can demonstrate compliance with consent requirements.

Data Subject's Rights and Requests

Data Subjects have rights when it comes to how the College handles their personal data. These include rights to:

- withdraw consent to processing at any time;

- receive certain information about the Data Controller's Processing activities
- request access to their personal data that the College holds
- prevent use of their personal data for direct marketing purposes
- ask for their personal data to be erased if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- restrict processing in specific circumstances
- challenge processing which has been justified on the basis of legitimate interest or in the public interest
- request a copy of an agreement under which personal data is transferred outside of the European Economic Area (EEA)
- object to decisions based solely on Automated Processing, including profiling
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms
- make a complaint to the supervisory authority
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

Staff must verify the identity of an individual requesting data under any of the rights listed and must forward any Data Subject requests received to the DPO immediately.

Subject Access Request (SAR) - A request to access personal information is known as a SAR. A request can be made by emailing info@qmc.ac.uk and marking the communication as a Subject Access Request and/or GDPR enquiry. Generally, there is no fee for a SAR and the College will respond within one month.

Commitment

The College is committed to maintaining the principles and duties in the GDPR at all times. Therefore the college will:

- Inform individuals of the identity and contact details of the data controller
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected for and the basis for this
- Inform individuals how their information is shared, and why and with whom unless the GDPR provides a reason not to do this (see also privacy statement).
- If the College plans to transfer personal data outside the EEA the College will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the College will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the College decide to use an individual's personal data for a different reason to that for which it was originally collected, the College will inform the individual and, where necessary, seek consent

- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whether stored on paper or electronically.
- Ensure that clear and robust safeguards are in place to ensure personal data is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (Subject Access Requests).
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards.
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Sharing Personal Data

The College will only share Personal Data with specified third parties and will ensure that safeguards and contractual arrangements have been put in place.

College staff will only share any personal information held about an individual with another member of staff if the recipient has a job-related need to know.

Personal data will only be shared with third parties, such as service providers, if:

- They have a need to know the information for the purposes of providing the contracted services.
- Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained.
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.
- The transfer complies with any applicable cross border transfer restrictions.
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.
- For child protection purposes.

Retention of Data and Disposal of Data

Personal data should not be retained beyond its useful time. The College will archive and store formal records held in central files for the periods of time indicated below. Other data maintained by staff should either be added to the formal records, or be destroyed within two years of the individual (staff or student) leaving the College.

Student Data

In general, student information will be kept for a maximum of seven years after they leave unless there are specific requests from the data subject to keep information for longer. This will include:

- name, address and contact details
- date of birth, health and ethnicity details
- academic progress records, including attendance, coursework marks, exam achievements and disciplinary matters
- copies of academic/employment references

Type of Data	Retention
Applicant Data (paper based or online)	7 years unless the applicant does not enrol in which case data will be kept for no more than 6 months (except in child protection cases)
Enrolment Data (paper based or online)	7 years
Child Protection Data	Until the child's 25th birthday

Staff Data

In general, staff information will be kept for seven years after a member of staff leaves. Some information however will be kept for much longer – this includes information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

Type of Data	Retention
Paperwork about unsuccessful job applicants	6 months
Staff personal record	7 years after date of leaving
Staff pay records (including tax and NI)	7 years after date of leaving
Staff term of service and pension records	40 years
Health records where there is any possibility that health could be a factor in leaving or success	7 years
Health records relating to COSHH incidents or any H&S incident/investigation	40 years

Disposal Procedures

It is essential that personal data is disposed of correctly once it is no longer required. In particular, paper records should be shredded on site and the College's certified waste contractor engaged to incinerate the material.

Computer records and files should be erased or rendered inaccessible unless transferred to the formal records as described above. From a practical point of view, records will be held on computer backup media for some considerable time (for example until the magnetic tapes are destroyed) but these data sets are only available to specialist personnel for the purposes of restoring selected data in the event of system reboot; they are not available for general purposes.

Direct Marketing

The College must abide by rules and privacy laws when marketing to customers. For example, a Data Subject's prior consent is required for electronic direct marketing (by email, text or automated calls). The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a Data Subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Privacy by Design and Data Protection Impact Assessment (DPIA)

The College must consider Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures to ensure compliance with data privacy principles.

The College must also conduct DPIAs in respect to high risk processing, for example, when implementing a new system, or changing an existing one, involving the processing of personal data.

Transfer Outside the European Economic Area

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the Information Commissioner's Office and, in certain instances, the Data Subject. The College has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where it is legally required to do so.

If an individual suspects that a Personal Data Breach has occurred they should contact the DPO immediately.

Complaints

Complaints will be dealt with in accordance with the College's Complaints Policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at ico.org.uk.

Review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulations.

Please follow this link to the Information Commissioner's Office website ico.org.uk which provides further detailed guidance on a range of topics including individuals' rights, exemptions, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection, which is available from the website.

Appendix to GDPR Policy

Definitions

Automated Processing: Any form of automated processing of Personal Data to evaluate certain personal aspects relating to an individual, eg, Profiling is an example of Automated Processing. The College does not process data in this way.

Consent: An agreement, which is freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the processing of Personal Data relating to them.

Data Controller: The person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. The College is the Data Controller of all Personal Data relating to its students and staff.

Data Subject: A living, identified or identifiable individual about whom we hold Personal Data.

Data Processor: Any person at the College or a third-party nominated to act on behalf of the College that is engaged in any activity that involves the use of Personal Data, for example collecting, storing, organising, amending, retrieving, disclosing, erasing or destroying, or carrying out any operation on the data. Processing also includes transmitting or transferring Personal Data to third parties.

Data Privacy Impact Assessment (DPIA): An assessment tool used to identify and reduce the risk of processing data. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business changes involving the Processing of Personal Data.

Data Protection Officer (DPO): The person with responsibility for data protection compliance.

EEA: The 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Personal Data: Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, identification number, location data, or by a person's physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Personal Data Breach: Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notices: Separate notices setting out information that may be provided to Data Subjects when the College collects information about them.

Pseudonymisation: Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information, which is meant to be kept separately and secure. For example, Student Number, or Staff Number

Sensitive Personal Data: Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

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		✘	