

DATA PROTECTION POLICY

The College is committed to the equality of opportunity and to a proactive approach to equality, which supports and encourages under-represented groups, promotes inclusivity and values diversity.

Responsible Senior Leader	CFO & Associate Principal (Finance, Estates & Risk)
Policy Owner	MIS Manager
Approved by	ELT
Approval date	December 2025
Next approval date	December 2028
Policy location	MIS and Exams Hub

Equality Impact Assessment by	Associate Principal (Learning and People Strategy)							
Intended Audience	Staff	X	Governors	X	Students	X	External	
Added to College website by						Date		
Added to Staff intranet by						Date		

Amendment summary

<u>Version no.</u>	<u>Date</u>	<u>Comments</u>	<u>Paragraphs amended</u>
1	2024.05.17		
2	2025.11.28	<p>'Learner' amended to 'student' throughout and 'personnel' to 'staff/employee' for consistency</p> <p>Legal name of the organisation corrected</p> <p>Clarified that this applies only to data sharing</p>	<p>1.1</p> <p>4.3</p>

The College is committed to the equality of opportunity and to a proactive approach to equality, which supports and encourages under-represented groups, promotes inclusivity and values diversity

Data Protection Policy

1 Introduction

- 1.1 WQE and Regent College Group (WQE) is committed to a policy of protecting the rights and privacy of individuals, including students, staff and others, in accordance with the Data Protection Act 2018, which is the UK's implementation of the General Data Protection Regulation (GDPR).
- 1.2 We will ensure that our privacy notices are written in a clear, plain way that staff and students will understand and that they provide the necessary information required under GDPR.
- 1.3 WQE needs to process certain information about its staff, students, parents and guardians and other individuals with whom it has a relationship for various purposes such as, but not limited to:
 - The recruitment and payment of staff.
 - The administration of programmes of study and courses.
 - Student enrolment.
 - Examinations and external accreditation.
 - Recording student progress, attendance and conduct.
 - Collecting fees.
 - Complying with legal obligations to funding bodies and government including local government.
- 1.4 To comply with the GDPR and other legal obligations, WQE must ensure that all information concerning individuals is collected and used fairly, stored safely and securely, and not disclosed unlawfully to any third party.
- 1.5 College employees will receive a copy of this policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any member of the employee's contract of employment and the College reserves the right to change this Policy at any time. All College employees are obliged to comply with this Policy at all times.

2 Data Protection Principles

- 2.1 All College employees are required to follow the data protection principles set out in the GDPR and the Data Protection Act (2018). Namely:

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- 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.

Article 5(2) requires that:

- The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

3. Definition

3.1 Data is information that is stored electronically, on a computer, or in certain paper-based filing systems (e.g. personnel files).

3.2 Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal information.

3.3 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name and address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the DPA.

- 3.5 Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
- 3.6 Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
- 3.7 Processing is any activity that involves the use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring data to third parties.
- 3.8 Special Categories of Personal Data includes information includes racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or details of any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special Categories of Personal Data can only be processed under strict conditions defined by Article 9 of the GDPR.

4. Compliance

- 4.1 This policy applies to all staff and students of WQE. Any breach of this policy or of the Regulation itself is likely to be an offence and may trigger the College's disciplinary procedures.
- 4.2 Other agencies and individuals working with WQE and who have access to personal information, will be expected to read and comply with this policy.
- 4.3 Departments who are responsible for sharing data with with external bodies will take the responsibility for ensuring that such bodies sign a contract that will include an agreement to abide by this policy and to ensure a robust data sharing agreement is in place.
- 4.4 This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

5. Responsibilities under the GDPR

- 5.1 WQE is the 'data controller' and is responsible for controlling the use of and processing of personal data.
- 5.2 WQE will ensure that all personal data is accessible only to those who have a valid reason for using it.
- 5.3 WQE will not transfer data outside of the UK or the European Economic Area (EEA) without the explicit consent of the individual.
- 5.4 WQE will have appropriate security measures and procedures to ensure that all electronic and hard copy personal data is kept secure.
- 5.5 WQE will put in place appropriate measures for the deletion or destroying of personal data in accordance with the Data Retention and Disposal Policy.
- 5.6 The Data Protection Officer (DPO) is available to address any concerns regarding the

data held by college and keeps the college's registration up-to-date. Our data registration number is Z6508135.

5.7 The Executive Leadership Team is responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the college.

5.8 Compliance with the GDPR is the personal responsibility of all members of the College who process personal information.

5.9 All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

5.10 All staff and students who provide personal data to the College are responsible for ensuring that the information is accurate and up-to-date.

6. The Rights of Individuals

GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children). Individuals who are the subject of personal data have a right to access the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request' (SAR).

6.1 For more detailed information on these regulations, see the Data Protection Data Sharing Code of Practice (DPCoP) from the [Information Commissioner's Office](#) (ICO).

6.2 The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

6.3 WQE will ensure that procedures and processes are in place to enable compliance with these rights. WQE reserves the right to refuse an individual's request and is aware of the information it needs to provide when it does so. Any individual wishing to exercise their rights should apply in writing to the DPO.

6.4 The College reserves the right to charge an administration fee for SARs. Under the terms of the legislation, any such requests must be completed within one month, but may be extended in special circumstances.

7. Procedure for review

- 7.1 This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 2018.
- 7.2 There will also be a review of this policy and of all privacy notices every three years.
- 7.3 For help or advice on any data protection or freedom of information issues, please do not hesitate to contact:

The data protection team: DPO@wge.ac.uk

8. Associated documents

Privacy Policies: The College will share privacy notices with any individual from whom it collects personal data. These will also be available via the College's website. The College has adopted the following privacy notices:

Student Applicant
Enrolled Student
Bursary Applicant
Job Applicant
Staff
Governor

Personal Data Breach Procedure:

Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and College staff must comply with the College's Personal Data Breach Notification Procedure.

Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

9. Personal data must not be kept for longer than needed

- 9.1 Data Protection Laws require that the College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.
- 9.2 The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.
- 9.3 If College staff feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if College Personnel have any questions about this Policy or the College's Personal Data retention practices, they should

contact the Data Protection Officer for guidance.