Data Protection Policy

Policy name:	**Data Protection**
Procedure reference:	**Pol-DP-LC**
Created by:	**Data Protection Officer**
Approved by:	**Corporation**
Date of last review:	**May 2025**
Date of next review:	**May 2026**
Revision number:	**16**

This document is available in other formats including audio, Braille and other languages. The same applies to all material which is referenced within in it. For further assistance, please contact the Quality Department on 01925 494593 or email quality@wvr.ac.uk

Contents

1. About this Policy

This Policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles uses, transfers and stores Personal Data.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

2. Definitions

2.1 **College – Warrington & Vale Royal College**

2.2 **College Personnel** – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

2.3 **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it. A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

2.4 Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

2.5 **Data Protection Officer –** The College's Data Protection Officer is Laura Churchill and can be contacted at: lchurchill@wvr.ac.uk.

2.6 **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

2.7 **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

2.8 **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

2.9 **Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

2.10 **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.

A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

2.11 **Special Categories of Personal Data** – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

Note: Paragraph 0 defines Special Categories of Personal Data. Although not strictly Special Categories of Personal Data, criminal offence/convictions data is also subject to additional controls so it has been included in the definition above. As discussed above, stricter rules apply to the collection and use of this type of data.

3. College Personnel's General Obligation

3.1 All College Personnel must comply with this policy.

3.2 College Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

3.3 College Personnel must not release or disclose any Personal Data:

3.3.1 Outside the College, except to those third parties detailed in the Privacy Notices for Students, Staff or Governors; or

3.3.2 Inside the college to College Personnel not authorised to access the Personal Data, without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

3.4 College Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Personnel who are not authorised to see such Personal Data or by people outside the College.

3.5 If staff intend to change how they use Personal Data, the Data Protection Officer must be notified who will, in conjunction with the appropriate College Leadership Team member, decide whether the intended use requires amendments to be made to the lawful basis, privacy notices, Information Asset Register (IAR) and any other controls which need to apply. The relevant College Leadership Team member is responsible for applying the updates following agreement by the DPO.

3.6 Staff that access Personal Data must review and update it as necessary to ensure its accuracy is maintained.

3.7 Staff must comply with the College's mandatory training requirements relating to information security, including the completion of annual refresher training.

4. Data Protection Principles

Note: This paragraph details the principles relating to the processing of Personal Data that are contained in Article 5 of the GDPR.

4.1 When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

4.1.1 Processed lawfully, fairly and in a transparent manner. We are required to identify a lawful basis from Article 6 of the UK GDPR for each processing activity we undertake;

4.1.2 If the processing activity involves the use of special category personal data, the College must identify an additional lawful basis from Article 9 of the UK GDPR;

4.1.3 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

4.1.4 Adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

4.1.5 Accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;

4.1.6 Kept for no longer than is necessary for the purposes for which it is being processed; and

4.1.7 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.

4.1.8 These principles are considered in more detail in the remainder of this Policy.

4.1.9 In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

5. Lawful Use of Personal Data

Lawful purposes for processing ordinary Personal Data

5.1 The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in section 5. If the College changes how it uses Personal Data, the College record of processing activity (ROPA) will be updated and individual(s) may need to be notified about the change. Intended changes must be notified to the Data Protection Officer to determine whether their intended use requires amendments to be made and any other controls which need to apply. This would be determined in conjunction with the appropriate member of the College Leadership Team.

5.2 These are set out in Article 6 of the GDPR and are as follows (paraphrased):

- the use of the Personal Data is for the purposes of the legitimate interests of the Controller;
- the processing is necessary for the performance of a contract;
- the processing is necessary for compliance with a legal obligation;
- the processing is necessary in order to protect the vital interests of the individual or of another natural person;
- the processing is necessary for the performance of a task carried out in the public interest; and
- the individual who is the subject of the Personal Data has given consent for one or more specific purposes.

5.3 Because the College is a public body, it cannot rely on the lawful purpose of legitimate interests where the processing is in the performance of a task carried out in the public interest or in the exercise of official authority. Instead, it needs to rely on the processing being necessary for the performance of a task carried out in the public interest.

5.4 Using consent to make your use of ordinary Personal Data lawful:

There are strict requirements on how the College can use consent - consent needs to be specific, freely given and informed. Consent can also be withdrawn at any time meaning that the Personal Data can no longer be processed.

5.5 In addition, in terms of the College's relationships with its employees, ICO guidance has stated that consent is not available in an employer and an employee relationship. The reasoning behind this is that the relationship is imbalanced and so the employee cannot really refuse to give their consent. Similarly, the ICO has commented that, for similar reasons, public authorities such as Colleges will find it difficult to rely on their position of power (e.g. over students).

6. Transparent Processing – Privacy Notices

6.1 Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College has adopted the following privacy notices: Privacy Notice for Staff, Privacy Notice for Students, and Privacy Notice for Governors and General Privacy Notice.

6.2 If the College receives Personal Data about an Individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

6.3 If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If College Personnel therefore intend to change how they use Personal Data please notify the Data Protection Officer who will decide whether the College Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

7. Data Quality – Ensuring the use of accurate, up to date and relevant personal data

7.1 Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

7.2 All College Personnel that collect and record Personal Data shall ensure that the Personal Data is:
-Recorded accurately;
-Kept up to date;
-Limit the collection and recording to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

8. Personal Data from sources outside the College does not require staff to independently check the Personal Data obtained.

8.1 In order to maintain the quality of Personal Data, all College Personnel that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

8.2 The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The College has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the College responds to requests relating to these issues. Any request from an individual for the

amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

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 Personnel 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.

10. Data Security

The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

11. Data Breach

11.1 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 Personnel must comply with the College's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which College Personnel need to comply with in the event of Personal Data breaches.

11.2 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.

11.3 There are three main types of Personal Data breach which are as follows:

11.3.1 **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

11.3.2 **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

11.3.3 **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

12. Appointing contractors who access the college's Personal Data

12.1 If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

12.2 One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

12.3 Any contract where an organisation appoints a Processor must be in writing.

12.4 You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

12.5 GDPR requires the contract with a Processor to contain the following obligations as a minimum:

12.5.1 to only act on the written instructions of the Controller;

12.5.2 to not export Personal Data without the Controller's instruction;

12.5.3 to ensure staff are subject to confidentiality obligations;

12.5.4 to take appropriate security measures;

12.5.5 to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

12.5.6 to keep the Personal Data secure and assist the Controller to do so;

12.5.7 to assist with the notification of Data Breaches and Data Protection Impact Assessments;

12.5.8 to assist with subject access/individuals rights;

12.5.9 to delete/return all Personal Data as requested at the end of the contract;

12.5.10 to submit to audits and provide information about the processing; and

12.5.11 to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

12.6 In addition the contract should set out:

12.6.1 The subject-matter and duration of the processing;

12.6.2 the nature and purpose of the processing;

12.6.3 the type of Personal Data and categories of individuals; and

12.6.4 the obligations and rights of the Controller.

13. Individuals' Rights

13.1 GDPR gives individuals more control about how their data is collected and stored and what is done with it.

13.2 The different types of rights of individuals are reflected in this paragraph.

13.3 **Subject Access Requests**

13.3.1 Individuals have the right under the GDPR to ask the College to confirm what Personal Data they hold in relation to them and provide them with the data. The timescale for providing it is one month (with a possible extension if it is a complex request). Fees will not be charged for complying with the request.

13.4 **Right of Erasure (Right to be Forgotten)**

13.4.1 This is a limited right for individuals to request the erasure of Personal Data concerning them where:

13.4.1.1 the use of the Personal Data is no longer necessary;

13.4.1.2 their consent is withdrawn and there is no other legal ground for the processing;

13.4.1.3 the individual objects to the processing and there are no overriding legitimate grounds for the processing;

13.4.1.4 the Personal Data has been unlawfully processed; and

13.4.1.5 the Personal Data has to be erased for compliance with a legal obligation.

13.4.2 In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

13.5 **Right of Data Portability**

13.5.1 An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:

13.5.1.1 the processing is based on consent or on a contract; and

13.5.1.2 the processing is carried out by automated means

13.5.2 This right isn't the same as subject access and is intended to give individuals a subset of their data.

13.6 **The Right of Rectification and Restriction**

13.6.1 Finally, individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

13.7 The College will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights in accordance with the College's Rights of Individuals Policy.

14. Marketing and Consent

14.1 The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner. Any electronic messages sent by the College, use of website cookies, or the provision of electronic communication services to the public must be done in accordance with the Privacy and Electronic Communications Regulation ('PECR').

14.2 Any colleagues engaging in direct marketing activities are required to seek consultation and approval from the DPO prior to commencing such activities.

14.3 Consent of the data subject is generally required for any electronic direct marketing.

14.4 An exception is made for the 'soft opt-in' rule, which allows the College to undertake direct marketing if:

14.4.1 We obtained contact details in the course of an enquiry to our services where we are marketing similar products or services;

14.4.3 We gave the individual the opportunity to opt out of marketing when first collecting their details; and

14.4.4 We give the individual the opportunity to opt out of marketing in each subsequent correspondence.

14.5 Data subjects have an absolute right to object to direct marketing, meaning that, if they do so, the College must not continue to engage in direct marketing to the data subject under any circumstances.

14.6 If a data subject objects to direct marketing, the College is permitted to keep sufficient personal data to ensure that we do not direct market to them again. This is known as suppression.

15. Automated Decision Making and Profiling

Automated Decision Making happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

15.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to individuals.

15.2 If staff wish to carry out any Automated Decision Making or Profiling the Data Protection Officer must be informed and approval provided before commencement.

15.3 The College does not carry out Automated Decision Making or Profiling in relation to its employees.

15.4 Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

15.5 Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If College Personnel therefore wish to carry out any Automated Decision Making or Profiling College Personnel must inform the Data Protection Officer.

15.6 College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

15.7 The College does not carry out Automated Decision Making or Profiling in relation to its employees.

16. Data Protection impact assessments (DPIA)

16.1 The UK GDPR mandates that a risk assessment must be carried out in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (**"DPIA"**). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

16.1.1 describe the collection and use of Personal Data;

16.1.2 assess its necessity and its proportionality in relation to the purposes;

16.1.3 assess the risks to the rights and freedoms of individuals; and

16.1.4 the measures to address the risks.

16.2 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals.

16.3 Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

16.4 Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

16.5 Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

16.5.1 large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;

16.5.2 large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

16.5.3 systematic monitoring of public areas on a large scale e.g. CCTV cameras.

16.6 All DPIAs must be reviewed and approved by the Data Protection Officer.

17. Data Sharing

17.1 The College must not share personal data with third parties unless certain safeguards and contractual agreements have been put in place.

17.2 The College must not share personal data with third parties unless the sharing is strictly necessary for the purposes of processing.

17.3 Personal data must only be shared with third parties if:

- The recipient is required to process the personal data to achieve the purposes of processing;
- Sharing the personal data complies with the privacy notice provided to the data subject;
- The recipient has agreed to comply with the required data security standards, policies and procedures, and has adequate security measures in place;
- The transfer of data complies with applicable cross border transfer restrictions; and
- A fully executed contract containing data protection clauses has been obtained and approved by the DPO.

17.4 Under certain circumstances, a data sharing agreement might also be required

17.5 Data sharing agreements are primarily required where multiple controllers are processing the same personal data, either independently or as joint controllers.

17.6 Any sharing of personal data with third parties must be logged on the ROPA.

17.7 Any colleagues who believe that a third-party personal data transfer may be taking place without the above provisions must contact the DPO as soon as possible.

18. Transferring Personal Data to a country outside the EEA

18.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

18.2 So that the College can ensure it is compliant with Data Protection Laws College Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

18.3 College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

Equality Impact Assessment

Policy Title:	Data Protection Policy

Identify the Key Stakeholders:	College staff, students and third parties with whom the college shares personal data	
What is the impact on the following:	**Key Characteristics**	**Impact**
	Age	(1) A positive impact is intended and very likely
	Disability	(1) A positive impact is intended and very likely
	Sex	(1) A positive impact is intended and very likely
	Racial group	(1) A positive impact is intended and very likely
	Religion and belief	(1) A positive impact is intended and very likely
	Sexual orientation	(1) A positive impact is intended and very likely
	Gender re-assignment	(1) A positive impact is intended and very likely
	Pregnancy and maternity	(1) A positive impact is intended and very likely
	Marriage and civil partnership	(1) A positive impact is intended and very likely

	Please tick			
Have any additional safeguarding risks been identified?	Yes	☐	No	☑
Any major changes or adjustments required:	Yes	☐	No	☑
Stop and remove:	Yes	☐	No	☑

Actions to be addressed:

Action	To be completed by	Target Date	Completed (Y/N)

Validated by the Equality & Diversity Committee **Date:**

If applicable, actions completed and validated by the Equality & Diversity Committee **Date:**