UK GDPR Policy

For the attention of:	All Staff
Produced by:	Group Principal and CEO
Approved by:	SLT/Board of Governors
Date of publication:	January 2026
Date of next review:	January 2028

WINDSOR FOREST COLLEGES GROUP

Vision, Purpose & Values

Our Vision

Our students will be recognised locally & nationally for their positive impact on the communities and industries in which they choose to work.

Our Purpose

To inspire our students to gain the skills, knowledge and behaviours they need to be resilient and thrive in an ever-changing world.

Our Values

Excellence: A culture of creativity, high expectations, ambition and aspiration

Respect: Showing fairness, courtesy and mutual respect to each other and our environment

Integrity: Honesty, openness and trust at the heart of College life

Diversity: Celebrating diversity and inclusivity as a key to our success

Contents

1. Overview

1.1. The Windsor Forest Colleges Group's (the College's) reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.

1.2. As an organisation that collects, uses and stores Personal Data about its employees, employers, suppliers (sole traders, partnerships or individuals within companies), students, governors, parents, customers and visitors, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of UK GDPR.

1.3. The College has implemented this Data Protection Policy to ensure all College Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

1.4. College Personnel will be asked to read this Policy and there will be periodic revisions of this Policy. This Policy does not form part of any member of the College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All members of College Personnel are obliged to comply with this Policy at all times.

1.5. If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the College's compliance with this Policy.

2. About This Policy

2.1. 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.

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

3. Definitions

3.1. College – The Windsor Forest Colleges Group.

3.2. **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.

3.3. **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.

3.4. **Data Protection Laws** – The UK GDPR, Data Protection Act 2018, subsequent Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, Data (Use and Access) Act 2025 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..

3.5. **Data Protection Officer –** The College's Data Protection Officer is Yee Har Miller, and can be contacted at: 01753 793000 or by email at data.protection@windsor-forest.ac.uk.

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

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

3.8. **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 suppliers such as partnerships and sole traders.

3.9. **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.

3.10. **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. Processing is any action taken with an individual's information, including storage, sharing, retrieval, using or erasing of Personal Data.

3.11. **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.

4. College Personnel's General Obligations

4.1. All College Personnel must comply with this policy.

4.2. 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.

4.3. College Personnel must not release or disclose any Personal Data unless there is a valid reason:

- outside the College; or
- 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.

4.4. 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

5. Data Protection Principles

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

5.1.1. processed lawfully, fairly and in a transparent manner;
5.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
5.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
5.1.4. 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;
5.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and
5.1.6. 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.

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

5.3. 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.

6. Lawful Use of Personal Data

6.1. In order to collect and/or use Personal Data lawfully the College needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing].

6.2. In addition when the College collects and/or uses Special Categories of Personal Data, the College has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/#:~:text=Special%20category%20data%20is%20personal,for%20processing%20under%20Article%209.

6.3. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 2.

6.4. In most cases the legal grounds for the College processing Personal Data is because:

6.4.1. the processing is necessary for the College to perform its contract with an Individual or

6.4.2. the processing is necessary for the College to comply with a legal obligation; or

6.4.3. the processing is necessary for the performance of a task carried out in the public interest.

6.4.4. the processing is necessary for the health / safety of the Individual and thus processed under vital interest.

6.4.5. The processing is necessary for the purposes of legitimate interest where the other legal grounds may not be applied

6.5. Otherwise, the College will seek the Individual's consent to process their Personal Data for a particular purpose.

6.6. The College sets out the legal grounds for processing in the privacy notices on its website and in the enrolment form for students.

6.7. If the College changes how it uses Personal Data, the College needs to update these records and may also need to notify Individuals about the change. If College Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

7. Transparent Processing – Privacy Notices

7.1. 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: General Privacy Notice, Privacy Notice for Students, Privacy Notice for Staff, Privacy notice for Governors.

7.2. 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.

7.3. 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.

8. Data Quality – Ensuring the Use of Accurate, up to Date and Relevant Data

8.1. 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 (see paragraph 7 above) 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.

8.2. All College Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

8.3. All College Personnel that obtain Personal Data from sources outside the College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require College Personnel to independently check the Personal Data obtained.

8.4. 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).

8.5. 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. 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 guidelines issued by the ICO.

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

10.1. 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 Prevention and Response Plan. Paragraphs 11.2 and 11.3 what could be deemed as Personal Data breaches. Please familiarise yourself with it as it contains important obligations which College Personnel need to comply with in the event a breach.

11.2. A Personal Data breach is defined as 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. Personal Data breaches can happen as a result of action taken by a third party, but they can also occur as a result of actions, whether intentional or accidentally, by College Personnel.

11.3. There are three main types of Personal Data breach:

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 ransomware, 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 UK GDPR is that a Controller must only use Processors who meet the requirements of the UK 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 yours or other individuals' 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 or share Personal Data without the Controller's instruction;
12.5.3. to ensure the Processor's employees are subject to confidentiality obligations;
12.5.4. to have appropriate data 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 if an incident occurs;
12.5.8. to assist with Data Protection Impact Assessments;
12.5.9. to assist with subject access requests or other requests relating to individuals' rights;
12.5.10. to delete/return all Personal Data as requested at the end of the contract;
12.5.11. to submit to audits and provide information about the processing; and
12.5.12. to tell the Controller if any instruction is in breach of the UK GDPR 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. Individual's Rights

13.1. UK data protection laws give individuals more control about how their data is collected and stored and what is done with it. It is extremely important that Colleges have a procedure in place detailing how they will handle these requests.

13.2. The different types of rights of individuals are detailed in this section.

13.3. Right of Access (Subject Access Requests)

13.3.1. Individuals have the right under UK data protection laws to ask a 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 calendar month or 30 calendar days (with a possible extension of up to three months in total if it is a complex request). The College will not be able to charge a fee for complying with the request but an administration fee may be considered under certain conditions.

13.3.2. Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

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:

13.4.2. the use of the Personal Data is no longer necessary;

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

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

13.4.5. the Personal Data has been unlawfully processed; and

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

13.4.7. 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:

13.5.2. the processing is based on consent or on a contract; and

13.5.3. the processing is carried out by automated means

13.5.4. This right is not the same as the right of access and is intended to give individuals a subset of their data.

13.6. The Right of Rectification and Restricted Processing

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.

13.6.2. 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 this regard. Please familiarise yourself with these

documents as they contain important obligations which College Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

14. Marketing and Consent

14.1. The College will sometimes contact Individuals to send them marketing or to promote the College's services. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

14.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. When the College undertakes any direct marketing it will ensure that:

14.3. It provides appropriate detail to individuals in our privacy notices, including for example whether profiling takes place; and

14.4. It will operate on an 'opt-in' basis when seeking consent to continue receiving direct marketing communications.

14.5. Personnel conducting marketing activities also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that applies to all forms of electronic communications for marketing and work alongside UK GDPR.

14.6. Alternatively, the College may be able to market using a "soft opt in" if the following conditions were met:

14.7. contact details have been obtained in the course of a sale (or negotiations for a sale);

14.8. the College are marketing its own similar services; and

14.9. the College gives the individual a simple opportunity to opt out of the marketing, both when first collecting the details and in every message after that.

15. Automated Decision Making and Profiling

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

15.2. 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

15.3. Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

15.4. 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, they must inform the Data Protection Officer. At present the College does not carry out any automated decision making or profiling on individuals.

15.5. College Personnel must not carry out Automated Decision Making or Profiling without first consulting with the Data Protection Officer.

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

15.7. Use of Artificial Intelligence for Content Assessment and Initial Responses

The College makes limited and proportionate use of automated tools, including artificial intelligence (AI), to support the **management of incoming communications** (such as emails, calls, digital messages and online enquiries).

These tools may be used to:

- assess the **general intent** of a communication (for example, whether it is an enquiry, complaint, request for support or general information);
- identify **sentiment or indicators of distress**, including potential safeguarding concerns;
- identify **security, abuse or threat-related content** requiring prioritisation or escalation; and
- generate **initial responses to routine or low-risk enquiries**, based on approved information, templates and knowledge sources.

AI-generated responses are used to provide **timely acknowledgement, information or signposting**, and are intended to support service efficiency and accessibility.

The College confirms that:

- **No automated decision-making with legal or similarly significant effects** is carried out.

- AI-generated responses do **not** determine outcomes, eligibility, disciplinary action, academic decisions, or safeguarding conclusions.
- **Human oversight is always maintained**, particularly where:
  - a message indicates distress, vulnerability, safeguarding or risk;
  - a complaint, escalation or adverse issue is identified; or
  - a response could materially affect an individual.

Where AI is used to generate responses:

- responses are constrained by **pre-defined rules, safeguards and knowledge sources**;
- high-risk, sensitive or ambiguous messages are **referred to human staff for review and response**;
- individuals may request **human review or intervention** at any point.

The College does **not** use AI for:

- behavioural prediction or scoring;
- profiling individuals for decision-making purposes; or
- making decisions without meaningful human involvement.

16. Data Protection Impact Assessment

16.1. Data Protection laws require the College to carry out a risk assessment 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 practically possible in the design of a new product/service/process. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- 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. The ICO's standard DPIA template is available from www.ico.org.uk.

16.3. Where a DPIA reveals risks which are not appropriately mitigated the ICO will 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, e.g. the use of high volumes of health data or Personal Data relating to criminal convictions and offences; 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. Transferring Personal Data to a Country Outside the UK or EU

17.1. Data Protection Laws impose strict controls on Personal Data being transferred outside the UK or EU/EEA states covered by GDPR, as some other countries' data protection laws may not be considered by UK lawmakers to be adequate in terms of protection of the data rights of UK individuals. Transfers may be the sending of Personal Data outside the UK but also includes storage of Personal Data or access to it outside the UK. It needs to be thought about whenever the College appoints a supplier outside the UK or the College appoints a supplier with group companies outside the UK which may give access to the Personal Data to staff outside the UK.

17.2. So that the College can ensure it is compliant with Data Protection Laws College Personnel must not transfer Personal Data outside of the UK or EU unless it has been approved by the Data Protection Officer.

17.3. College Personnel must not export any Personal Data outside the UK or EU/EEA without the approval of the Data Protection Officer.

18. Scope and Limitations

18.1. The policy covers all aspects of personal data that is identifiable.

18.2. Retention of Records

18.3. The College has a legal requirement to hold data for a range of reasons and is a requirement of certain legal bodies including but not limited to Government Funding Organisations and HM Revenue & Customs.

18.4. The Data Retention Policy states what data the College holds and how long each different type of data will be kept for.

18.5. At the end of the retention period the data will be disposed of securely following the College procedures.

18.6. CCTV

18.7. CCTV is recorded for safeguarding and security requirements on all College sites. Notices are clearly displayed on the entrance to all sites. Data is kept for a maximum of 31 days, unless the data has been requested for an on-going incident or accident, in which case it will be kept until 6 months after the case is closed.

18.8. CCTV can only be accessed by specific authorised staff.

18.9. Further details can be found in the CCTV Policy.

18.10. Photography

18.11. Photography for any purpose other than ID badges or Staff posters will require explicit consent from an individual.

18.12. Consent will be obtained during the enrolment process and stored on the College MIS system.

18.13. The marketing team and associated contractors will get explicit consent for any marketing activities.

18.14. Staff undertaking trips or visits will obtain a list from the MIS system listing students who have consented to having their photo taken. Students who have opted out will get an additional form signed if they intend to use an image of that individual.

18.15. As part of open events and general photography, signs must be clearly visible and guidelines followed from the Digital Images Procedures.

18.16. Financial Data

18.17. Financial Data, particularly credit card payments will be taken securely to comply with the Payment Card Industry Data Security Standard (PCI DSS).

18.18. Disclosing to Parents

18.19. Data will not be disclosed to parents without explicit consent from the student. This will be given on the enrolment form or in the case of an online ILP system the student giving access to the parent.

18.20. Exceptions to this are where the individual is not legally competent to understand their own data. Learners over the age of 13 will be appropriately assessed for competency in their understanding and the College will make a judgement accordingly.

19. Responsibilities

19.1. It is the responsibility of all staff to ensure that all data within the college is held in accordance with UK GPDR guidance.

19.2. The Governing body and Senior Leadership Team are responsible for ensuring that there is the required policy and framework in place to ensure the college is compliant with UK GDPR.

19.3. The Data Protection Officer is responsible for developing the policies, ongoing monitoring of compliance with UK GDPR within the College, recording any breaches and raising awareness across the college to support compliance.

19.4. There are specific areas of the college that hold a large amount of personal data and the responsibilities for each area and person responsible for ensuring compliance and control of data in each of these areas:-

19.5. Human Resources (Staff Data)– Group Executive Director of People

19.6. Student Information (Student Data) – Group Head of MIS

19.7. Examinations (Student Data) – Group Head of MIS / Group Exams Manager

19.8. Finance (Staff and Student Data) – Group Director of Finance

19.9. IT (Security of systems and Data for staff and students) – Head of IT Infrastructure and Security

19.10. Estates (Disposal of secure waste and CCTV) – Directors of Estates

20. Privacy Notice and Website

20.1. The College will publish and update via its website, the College's Privacy notices and the Policies relating to data protection.

20.2. Students and Staff when starting at the College will be provided with the College's privacy notices and have the option of opting in or giving consent for any items not covered by a legal requirement to process.

21. Complaints Management Process

21.1. Any individual can make a complaint regarding the way their data is processed, or the way their data request has been handled by writing to the DPO, at data.protection@windsor-forest.ac.uk.

21.2. If they believe that the complaint has not been resolved successfully and wish to escalate the complaint then students and external bodies can use the College's normal complaints procedure, by writing to complaints@windsor-forest.ac.uk. The College's complaints procedure can be found on the staff intranet and on the College website.

21.3. The final stage of escalation of a personal data complaint is to contact the Information Commissioner's Office at https://ico.org.uk/make-a-complaint/ and complete the online complaint form.

22. Information Asset Register

22.1. The college's information asset register lists all data that is held by the college, where it is stored and the area responsible. This list will continue to be updated as new software or data is stored and kept as an up-to-date list. This information is key when the college receives a Subject Access Request as it will identify all data held and where to access the data to ensure the college fully complies with any request.

23. Data Sharing Agreements

23.1. The college through contracts has a number of Data Sharing Agreements in place. These fall into 4 main categories:-

- Suppliers of systems and services
- Sub-contractors
- Awarding Bodies and HE institutions
- Other organisations we share data with

23.2. UK GDPR and data sharing agreements will be written into all contracts and variations to contracts issues for existing contracts.

23.3. The first 3 categories fall under business interests to share data. Any contracts issued under the category Other Organisations will require a Data Sharing Agreement unless they have a regulatory obligation to obtain the data e.g. progression data for schools.

23.4. The process and approval of data sharing is managed by the DPO. Any enquiries regarding data sharing requests should be sent to the DPO at data.protection@windsor-forest.ac.uk.

24. Recordof Processing Activity (RoPA)

24.1. The RoPA details the responsibilities of staff and areas for the recording, usage, storage and disposal of personal data across the college. This is in conjunction with the Information Asset Register, which shows all data stored by area and the rights under GDPR for processing and owner.

25. Monitoring and Review

25.1. The compliance of the policy and regular review will be undertaken in a number of ways to mitigate the risk of data breaches.

25.2. Log of all data protection requests and breaches to be held by the Data Protection Officer

25.3. Regular checks on all staff that they have completed the mandatory annual data protection training by the data protection officer

25.4. Termly internal audit reviews a year based on high risk areas within the college to be undertaken by the data protection officer and written feedback and changes to be given

25.5. Annual reporting to SLT and Board on training, current issues and risks from audits, contingency measures and any breaches from the data log

26. Associated Documents

- Privacy and Cookies Policy
- Data Breach Prevention and Response Plan
- IT Security Policy
- Cyber Security Policy

- Student BYOD Policy
- Wearable Technology Policy
- Wireless Networking Policy
- IT Acceptable Usage Policy
- Data Retention Policy and Procedures
- Privacy Notices
- Encryption Policy
- Information Asset Register
- CCTV Policy
- Social Media Policy
- Use of AI by Staff policy
- IT Disaster Recovery Plan