EAST SUSSEX COLLEGE

GDPR Policy

Policy Area:	**General Corporate**
Policy Lead:	**Director of MIS & Digital**
Approved By:	**Governing Board**
Date of Approval:	**July 2023**

Contents

1. Overview

1.1. 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, suppliers (sole traders, partnerships or individuals within companies), students including potential students, governors, parents 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 GDPR.

1.3. The college has implemented this Data Protection Policy to ensure all staff 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 staff will receive a copy of this policy when they commence employment and may receive periodic revisions of this policy. This policy does not form part of any member of staff's contract of employment and the college reserves the right to change this policy at any time. All members of staff are obliged to comply with this policy at all times.

1.5. If you have any queries concerning this policy, please contact the Data Protection Officer (data.protection@escg.ac.uk), 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 stored electronically, in paper form, or otherwise.

3. Definitions

3.1. College – East Sussex College Group.

3.2. College staff – 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.

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.

3.4. Data protection laws – covers the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018 and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by the ICO.

3.5. Data Protection Officer – the college's Data Protection Officer can be contacted at

data.protection@escg.ac.uk

3.6. 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.

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 this information can be used to reveal their identity. Individuals include staff, students, parents, visitors and potential students. Individuals also include 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 external software support for a system which contains personal data, cloud arrangements and mail fulfilment services.

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 staff's general obligations

4.1. All college staff must comply with this policy.

4.2. College staff 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 staff must not release or disclose any personal data:

4.3.1. Outside the college; or

4.3.2. Inside the college to college personnel not authorised to access the personal data,

4.3.3. Without specific authorisation from their manager or the data protection officer; this includes by phone calls or in emails.

4.4. College staff must take all steps to ensure there is no unauthorised access to personal data, whether by other college staff 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 is 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[1]. These are set out in Article 6 of the GDPR and are as follows (paraphrased):

6.1.1. The use of the personal data is for the purposes of the legitimate interests of the controller;

6.1.2. The processing is necessary for the performance of a contract;

6.1.3. The processing is necessary for compliance with a legal obligation;

6.1.4. The processing is necessary in order to protect the vital interests of the individual or of another natural person;

6.1.5. The processing is necessary for the performance of a task carried out in the public interest; and

6.1.6. The individual who is the subject of the personal data has given consent for one or more specific purposes.

6.2. In addition when the college collects and/or uses special categories of personal data, the

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

college has to show that one of a number of additional conditions is met[2]. These are set out in Article 9 and are as follows (paraphrased):

6.2.1. Explicit consent;

6.2.2. Employment and social security obligations;

6.2.3. Vital interests;

6.2.4. Necessary for establishment or defence of legal claims;

6.2.5. Substantial public interest; and

6.2.6. Various scientific and medical issues.

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 6.2. If the college changes how it uses personal data, the college needs to update this record and may also need to notify individuals about the change. If college staff therefore intend to change how they use personal data at any point they must notify the Data Protection Officer who will determine 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, it will inform them about how it their personal data. This information is in Privacy Notices (staff and student), copies of which are available on the college's intranet and website.

7.2. If the college receives personal data about an individual from other sources, it will provide the individual with a privacy notice about how it 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, it may need to notify individuals about the change. If a staff member intends to change how they use personal data they should notify the Data Protection Officer who will determine whether that 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 personal 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 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 it holds is accurate and kept up to date.

8.2. All college staff 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 staff 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

[2] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data

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 staff to independently check the personal data obtained.

8.4. In order to maintain the quality of personal data, all college staff 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.

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 Schedule.

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 schedule, for example because there is a requirement of law, or if they 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 has security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

10.2. 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. These are further detailed in the Network Security Guidelines.

11. Data breach

11.1. While the college takes information security very seriously, 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. this is a personal data breach and college staff must refer to the college's Data Breach Notification Policy.

11.2. A 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. While most personal data breaches happen as a result of action taken by a third party, they can also occur as a result of an internal error.

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 staff member is not authorised to access, accessing personal data stored on a lost laptop, phone or other device, a person obtaining by deception access to personal data they have no right to access, putting a 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. Any contractor/ or supplier who provides a service by using any personal data is considered a data processor.

12.2. Any processor of the college's personal data must only be appointed once the college has carried out sufficient due diligence and only when the college has appropriate contracts in place. These contracts must be in writing.

12.3. The college will only use processors who meet the requirements of the GDPR and protect the rights of individuals. Once a processor is appointed, they should be reviewed periodically to ensure that they are meeting the requirements of their contract in relation to data protection.

12.4. The college will retain the controller responsibility and remain responsible for what happens to the personal data.

12.5. Any contract with a processor must 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. The different types of rights of individuals are reflected in this paragraph. Please put any specific request or questions in writing to the Data Protection Officer.

13.2. Subject access requests

13.2.1. Individuals have the right to ask the college to provide them with copies of the personal data it holds in relation to them. This is commonly known as a subject access request or SAR.

13.2.2. The college will respond to a SAR within one month from the date it has been received. If the SAR is complex or there are multiple requests at once the college may extend this period by two further months. In this case the college will tell the individual who has made the SAR about the delay and the reasons for the delay within the first month.

13.2.3. In line with GDPR the college is not entitled to charge individuals for complying with this request. However, if the individual would like a further copy of the information requested, the college can charge a reasonable fee based on the administrative costs of making the further copy.

13.2.4. The Data Protection Officer will determine the complexity of the SAR and whether the college is entitled to extend the deadline for responding.

13.2.5. If the request is considered manifestly unfounded or excessive the college will refuse to respond to it.

13.2.6. Individuals have the right to complain to the ICO if they are unhappy about how the college has dealt with a request or in general about the way the college is handling their personal data.

13.3. Right of erasure (right to be forgotten)

13.3.1. This is a limited right for individuals to request the erasure of personal data concerning them.

13.3.2. At the college this generally only occurs in the cases where it has specifically collected personal data for direct marketing purposes.

13.3.3. The individual has the right to stop the processing for this purpose at any time.

13.3.4. Where the college uses electronic tools for this purpose there will be an opt-out or unsubscribe option available.

13.3.5. The college will respond to these requests within one month.

13.4. Right of data portability

13.4.1. An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format (usually Microsoft Excel), where:

13.4.1.1. The processing is based on consent or on a contract; and

13.4.1.2. The processing is carried out by automated means

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

13.4.3. The college will aim to respond to these requests within one month.

13.5. Right of rectification

13.5.1. Individuals also have the right to request that any personal data is rectified if inaccurate.

13.5.2. The college will respond to these requests within one month.

13.5.3. In certain circumstances the college can refuse these requests; if this is the case the college will provide a written explanation.

13.6. Right of restriction

13.6.1. In certain circumstances individuals have the right to request that their personal data is restricted to particular purposes (this will usually only occur if there is a dispute over the data).

13.6.2. The college will respond to these requests within one month.

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 these laws.

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, it will be undertaken in a legally compliant manner.

14.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. Generally the college will process this personal data under one of two legal bases - consent or legitimate interest:

14.3. Consent requires the use of a "clear affirmative action", usually in the form of an un-ticked opt-in box.

14.3.1. The college will use an un-ticked opt-in box or other means i.e. signing up for communications, to ensure consent is actively given.

14.3.2. Consent can be withdrawn at any time.

14.3.3. In ongoing communications the college will have an opt-out/unsubscribe option.

14.4. Legitimate interest may be used if the following conditions are met:

14.4.1. Contact details have been obtained in the course of a sale/enrolment (or negotiations for a sale/enquiry/application), and

14.4.2. The college is marketing its own similar services; and

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

14.5. The college's marketing team will ensure that they identify the basis of processing prior to undertaking any marketing activity.

14.6. Any individual's data that is reproduced for marketing purposes, for example use of images

and testimonials, will only be used once the college has received a completed consent form (physical or digital) for this purpose.

14.7. Alongside this the college will adhere to the Privacy and Electronic Communications Regulations (PECR) in its marketing communications. These regulations apply to electronic communication i.e. calls, emails, texts, faxes, and are upheld even if personal data is not being processed.

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 takes place when 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 takes place when the college automatically uses personal data to evaluate certain things about an individual.

15.4. Currently the college carries out no automated decision making or profiling.

15.5. If college staff wish to carry out any automated decision making or profiling they must refer to the Data Protection Officer.

16. Data Protection Impact Assessments (DPIA)

16.1. Where the college is launching or proposing to adopt a new service or a significant change to a process which involves personal data, the college will assess whether it needs to carry out a Data Protection Impact Assessment (DPIA). If required, this is should be undertaken at an early stage in the process.

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. The DPIA will seek to address issues that will need to be considered. The process is designed to:

16.3.1. Describe the collection and use of personal data;

16.3.2. Assess its necessity and its proportionality in relation to the purposes;

16.3.3. Assess the risks to the rights and freedoms of individuals; and

16.3.4. Assess the measures to address the risks.

16.4. College staff must complete the DPIA using the form available on the college's intranet.

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

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

17. Transferring personal data to a country inside the EEA

17.1. As of 28 June 2021 the EU has adopted an adequacy decision for transfer of personal data with the United Kingdom. The effect of such a decision is that personal data can flow between the EU (and Norway, Liechtenstein and Iceland) and the UK without any further safeguard being necessary.

18. Transferring personal data to a country outside the UK and 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. This must be considered if the college appoints a supplier either itself outside the EEA or if the supplier has group companies outside the EEA.

18.2. In these circumstances college staff must not export personal data without the approval of the Data Protection Officer.