Varndean College Polices and Procedures

Data Protection Policy

CONTENTS

1. OVERVIEW

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.

As an organisation that collects, uses and stores Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, governors and parents, 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.

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.

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

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.

College Personnel will be directed to this Policy when they start and may receive periodic revisions of this Policy. All members of College Personnel are obliged to comply with this Policy at all times. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any member of College Personnel who considers that the policy has not been followed in respect of personal data about themselves should initially raise the matter with the designated Data Protection Officer. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

3. DEFINITIONS

College – Varndean College Brighton & Hove

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

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.

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.

Data Protection Officer – Our Data Protection Officer is Elaine French, and can be contacted at: 01273 508011, dpo@varndean.ac.uk.

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.

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

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.

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.

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.

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 GENERAL OBLIGATIONS

All College Personnel must comply with this policy.

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.

College Personnel must not release or disclose any Personal Data:

- 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.

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

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

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

- 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.

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

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

It is essential that the collection and use of Personal Data is lawful. This means that any use of the Personal Data must fall within one of a number of "lawful purposes":

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For more detail on each lawful basis, click here https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

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, including:

- The Individuals have given explicit consent

- Processing is necessary for carrying out College obligations relating to employment or social security

- Processing is necessary to protect the vital interests of the Individual where they are physically or legally incapable of giving consent

- Processing is necessary for the defence of legal claims

- Processing relates to data which has been manifestly made public by the Individual

- Processing is necessary for statutory or legal reasons

- Please click here to see the detailed additional conditions https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data].

The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs **Error! Reference source not found.** and 0. If the College changes how it uses Personal
Data, the College must update this record 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. TRANPARENT PROCESSING – PRIVACY NOTICES

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

- Students
- Adult education students
- Staff
- Governors
- Parents
- Suppliers/other bodies
- Host families

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.

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 PERSONAL DATA

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 **Error! Reference source not found.** 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.

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.

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.

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).

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. Section 13 of this policy sets 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 this.

9. PERSONAL DATA MUST NOT BE KEPT LONGER THAN IS REQUIRED

The College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.

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.

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

Whilst 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. 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 below 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.

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.

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

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. deception, 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, 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;

- **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

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

12. APPOINTING CONTRACTORS WHO ACCESS COLLEGE PERSONAL DATA

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

The College has appointed a Processor where it engages someone to perform a service for you and as part of it they may get access to College Personal Data. As the Controller, the College remains responsible for what happens to the Personal Data.

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

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals rights;
- to delete/return all Personal Data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

In addition the contract should set out:

- The subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of Personal Data and categories of individuals; and
- the obligations and rights of the Controller.

13. INDIVIDUALS' RIGHTS

The College will ensure it allows individuals to exercise their rights in accordance with Data Protection Laws. The different types of rights of individuals are reflected in this section.

Subject Access Requests

Individuals have the right under the GDPR to ask a College to confirm what Personal Data they hold in relation to them and to have copies of that Personal Data along with the following information:

- the categories of their Personal Data and the purposes for which it is used
- the recipients or categories of recipients that their Personal Data will be disclosed to
- how long the College will keep their Personal Data
- that they have the right to request that the College corrects any inaccuracies in their Personal Data or deletes their Personal Data *(in certain circumstances, please see below for further information)* or restrict the uses the College is making of their Personal Data *(in certain circumstances, please see below for further information)* or to object to the uses the College is making of their Personal Data *(in certain circumstances, please see below for further information)*
- that they have the right to complain to the ICO if they are unhappy about how the College has dealt with this request or in general about the way the College is handling their Personal Data
- where the Personal Data was not collected from them, where the College got it from
- the existence of automated decision-making, including profiling (if applicable).

This must be provided within one month of the request. If the request is complex this period may be extended. Any extensions must be explained in writing to the Individual making the request.

The College Data protection Officer must be notified of all Subject Access Requests at the point the request is submitted.

Right of erasure (Right to be Forgotten)

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

- the use of the Personal Data is no longer necessary;
- their consent is withdrawn and there is no other legal ground for the processing;

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

- the Personal Data has been unlawfully processed; and

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

If the College has disclosed the individual's deleted Personal Data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties to delete the Personal Data where the College can.

When an individual asks the College to delete their Personal Data, the College is required to do so and to inform the individual in writing within one month of them making the request that this has been done.

Right to Restrict Processing

Individuals have the right to "block" or "suppress" the College's processing of their Personal Data when:

- they contest the accuracy of the Personal Data, for a period enabling the College to verify the accuracy of the Personal Data;

- the processing is unlawful and the individual opposes the deletion of the Personal Data and requests restriction instead;

- the College no longer needs the Personal Data for the purposes the College collected it for, but the College is required by the individual to keep the Personal Data for the establishment, exercise or defence of legal claims;

- the individual has objected to the College's legitimate interests, for a period enabling the College to verify whether its legitimate interests override their interests.

If the College has disclosed the individual's restricted Personal Data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties about the restriction where the College can.

When an individual asks the College to restrict its processing of their Personal Data, the College is required to do so and to confirm to the individual in writing within one month of them making the request that this has been done.

Right of Data Portability

Individuals have the right to obtain from the College a copy of their own Personal Data in a structured, commonly-used and machine-readable format (such as CSV files). The aim of this right is to facilitate the ability of individuals to move, copy or transmit their Personal Data easily from one IT environment to another.

The right to data portability only applies when:

- the individual provided the College with the Personal Data;
- the processing the College is carrying out is based on the individual's consent or is necessary for the performance of a contract; and
- the processing is carried out by automated means.

This means that the right to data portability does not apply to personal data the College is processing on another legal basis, such as its legitimate interests.

The College is obliged to provide this information free of charge within one month of the individual making the request (or two months where the request is complex provided that the College explains to the individual why it needs more time).

The individual also has the right to ask the College to transmit the Personal data directly to another organisation if this is technically possible.

The Right of Rectification

Individuals have the right to ask the College to correct any Personal Data about them that the College is holding that is incorrect. The College is then obliged to correct that Personal Data within one month (or two months if the request is complex).

Where the individual tells the College their Personal Data is incomplete, the College is obliged to complete it if the individual asks the College to do so. This may mean adding a supplementary statement to their personal file for example.

If the College has disclosed the individual's inaccurate Personal Data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties of the correction where the College can.

When an individual asks the College to correct their Personal Data, the College is required to do so and to confirm this in writing to the individual within one month of them making the request.

Right to object

Individuals have the right to object to the College's processing of their Personal Data where:

- the College's processing is based on its legitimate interests or the performance of a task in the public interest and the individual has grounds relating to his or her particular situation on which to object;
- the College is carrying out direct marketing to the individual; and/or
- the College's processing is for the purpose of scientific/historical research and statistics and the individual has grounds relating to his or her particular situation on which to object.

- If an individual has grounds to object to the College's legitimate interests, the College must stop processing their Personal Data unless the College has compelling legitimate grounds for the processing which override the interests of the individual, or where the processing is for the establishment, exercise or defence of legal claims.

- If an individual objects to direct marketing, the College must stop processing their Personal Data for these purposes as soon as the College receives the request. The College cannot refuse their request for any reason and cannot charge them for complying with it.

- Before the end of one month from the date the College gets the request, the College must notify the individual in writing that the College has complied or intends to comply with their objections or that the College is not complying and the reasons why.

Rights in relation to automated decision making

Automated decision making happens where the College makes a decision about an individual solely by automated means without any human involvement; and

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

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, unless the decision is:

- necessary for entering into or performing a contract between the College and the individual;

- required or authorised by Data Protection Laws; or

- based on the individual's explicit consent.

14. MARKETING AND CONSENT

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.

Where contact details have been obtained in the course of its normal business, individuals can be contacted in relation to relevant information about College services. The College will not share personal data with any other organisation for marketing purposes.

15. AUTOMATED DECISION MAKING AND PROFILING

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

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.

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.

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

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

16. DATA IMPACT ASSESSMENTS (DPIA)

A DPIA (Data Protection Impact Assessment) must be completed for any new project, prior to any processing, 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.

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:

- 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
- assess the measures to address the risks.

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

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):

- 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;

- 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

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

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

17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

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 will apply 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.

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

18. RESPONSIBILITIES

The Governing Body is responsible for ensuring the College has appropriate policies and procedures in place for Data Protection.

The Principal has responsibility for ensuring that these policies and procedures are fully implemented.

19. MONITORING

This policy will be reviewed every three years, or sooner if any changes to the General Data Protection Regulations and Data Protection Act 2018 are announced.

College Personnel will be made aware of this policy and should contact the Data Protection Officer for guidance where necessary. This Policy does not form part of any College Personnel's contract of employment and the College reserves the right to change this Policy at any time.

The College reserves the right to change this policy at any time.

20. RELATED POLICIES

- Data Retention Policy
- Data Breach Notification Policy
- IT Security policy