Data Protection Policy 2021-22

Lead Responsible:	Director of Management Information Systems & Admissions
Approval Dates for Revisions:	
Academic Board/College Leaders	
Equality Impact Assessment	
Governor Committee: AC/FR/AU/SG/ES	
Governing Body	
Effective Date:	September 2021
Annual Review Date:	Summer 2022
Original Filename:	Z:\Executive Support\VP\Policies\Data Protection Policy\2021-22\Data Protection Policy 2021-22.docx

Introduction

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.

2. As an organisation we collect, use and store Personal Data about our students, employees, governors, parents, visitors, suppliers, partnerships or individuals within companies. Capel Manor College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with our obligations under the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 (GDPR) and in particular our obligations under Article 5.

3. Capel Manor 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.

4. College Personnel will receive a copy of this Policy when they start employment and may receive periodic revisions of this Policy as considered appropriate. 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.

5. If you have any queries concerning this Policy, please contact the College Data Protection Officer, Richard Davies, who is responsible for ensuring the College's compliance with this Policy: dataprotection@capel.ac.uk

6. 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.

7. This policy applies to all Personal Data stored electronically, in paper form, or otherwise.

Policy Statement

8. All College staff must comply with this policy.

9. 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.

10. College staff must not release or disclose any Personal Data without specific authorisation from their manager or the Data Protection Officer either to those outside the College or to College staff not authorised to access such data.

11. College staff must take all necessary 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.

Data Protection Principles

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

1.12.1. processed lawfully, fairly and in a transparent manner;
1.12.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
1.12.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
1.12.4. 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;
1.12.5. kept for no longer than is necessary for the purposes for which it is being processed; and
1.12.6. 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.

13. In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them: this is the concept of Accountability.

14. Accountability requires compliance with the GDPR to be documented. It is not enough for the College to comply; the College must be able to demonstrate compliance through documentation.

15. The College has a number of policies and procedures in place, including this Policy and the documentation referred to within it, to ensure that the College can demonstrate its compliance.

Lawful Use of Personal Data

16. The College will ensure the collection and use of Personal Data will only be processed for "lawful purposes".

17. Lawful purposes for processing ordinary Personal Data (Article 6 of the GDPR) are:

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

18. Lawful purposes for processing Special Categories of Personal Data (Article 9 of the GDPR) are:

1.18.1. explicit consent;
1.18.2. employment and social security obligations;
1.18.3. vital interests;
1.18.4. necessary for establishment or defence of legal claims;
1.18.5. substantial public interest; and
1.18.6. various scientific and medical issues.

19. In order to collect and / or use Personal Data lawfully the College will ensure that its use meets one of a number of these legal grounds.

20. In addition when the College collects and / or uses Special Categories of Personal Data, the College will show that one of a number of additional conditions are met.

21. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out above.

22. Student Personal Data (enquirer, existing or previous students) will, generally, be processed as part of our public interest task of providing education. Where that information is special category personal information this will be processed for substantial public interest reasons.

23. Student Personal Data (enquirer, existing or previous students) for marketing purposes will be processed on the basis of either our legitimate business interests or on the basis of consent.

24. Student Personal Data for Alumni purposes will be processed on the basis of consent or business interest.

25. Staff Personal Data will be processed on the basis of performing an employment contract, complying with our legal obligations and the College's legitimate and public interest. Where that information is special category personal information this will be processed on the basis of our legal obligations, substantial public interest and in certain circumstances explicit consent and or to protect the vital interests of the individual concerned.

26. The Personal Data of visitors to the College will be processed on the basis of the College's legitimate interests. Where the College is required by law to hold certain records, then we will process this data on the basis of our legal obligation or consent.

27. The Personal Data of those chosen to supply services to the College will be processed on the basis of our legitimate interests, legal obligation and in the performance of a contract.

28. If the College changes how it uses Personal Data, the College will update its Privacy Statements and may also notify Individuals about the change, if appropriate.

29. If College staff 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 may need to apply.

Transparency

30. The College will be transparent on how we will use Personal Data through the publication of Privacy Statements. These will be written in a way that is easy to understand in clear plain language tailored, for its specific audience and in an accessible format.

31. These Privacy Statement will comply with and include the information as detailed within Article 13 and 14 of GDPR.

32. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. The College has adopted the following Privacy Statements:

33. General Privacy Statement: for visitors and our suppliers of services to our College.

34. Student Privacy Statement: for enquirer, existing students or previous students to our College.

35. Staff Privacy Statement: for those wishing to be employed by the College and staff who are either currently employed or have been employed by the College.

36. If the College receives Personal Data about an Individual not listed above, 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.

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

Data Quality & Accuracy

38. The College will only collect and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy statement (see Section 5 above).

39. The College will ensure that the Personal Data the College holds is accurate and kept up to date.

40. 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.

41. 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 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.

42. 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).

43. 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 will be dealt with in accordance with this policy.

Data Retention

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

45. 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 College Retention Policy.

46. 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 Retention Policy, for example because there is a requirement of law, or if College staff have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

47. Personal information (and sensitive personal information) that is no longer required will be deleted permanently from the College's information systems and any hard copies will be destroyed securely

Data Security

48. The College takes information security very seriously and has in place security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data.

49. 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.
50. Despite these procedures and technologies it may be possible for a security breach to take place which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data.

51. 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.

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

    1.52.1. **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 gaining 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;
    1.52.2. **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
    1.52.3. **Integrity breach:** where there is an unauthorised or accidental alteration of Personal Data.

53. If such a breach occurs and is likely to result in a risk to the rights and freedoms of individuals the Data Protection Officer will notify the Information Commissioner's Office (ICO) within 72 hours of the College becoming aware of the breach.

Appointing Contractors

54. The College will only appoint contractors who Process the College's Personal Data once sufficient due diligence has taken place and where appropriate contracts are in place.

55. The College will only appoint contractors who meet the requirements of the GDPR and protect the rights of individuals. Data protection due diligence will 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.

56. Any contract where the College appoints a Processor will be in writing.

57. Where the College has appointed a Processor, the College, as Controller, will remain responsible for what happens to the Personal Data.

58. The College will ensure that any contract with a Processor will contain the following obligations as a minimum:

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

59. The College will also ensure that any such contract will detail the:

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

60. For each contract, financial liability will be reviewed and set at an amount considered appropriate.

Individuals' Rights

61. The College, through adhering to the principles of GDPR will give individuals control about how their data is collected, stored and processed.

62. **Subject Access Requests**

1.62.1. Individuals will have the right to ask the College to confirm what Personal Data they hold in relation to them and provide them with the data. The College will provide this data within one month of receiving a written request and will not charge a fee for complying with the request.

63. **Right of Erasure (Right to be Forgotten)**

1.63.1. Individuals will have the right to request the erasure of Personal Data concerning them where:
1.63.2. the use of the Personal Data is no longer necessary;
1.63.3. their consent is withdrawn and there is no other legal ground for the processing;
1.63.4. the individual objects to the processing and there are no overriding legitimate grounds for the processing;
1.63.5. the Personal Data has been unlawfully processed; and
1.63.6. the Personal Data has to be erased for compliance with a legal obligation.
1.63.7. 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 will not be processed for such purposes.

64. **Right of Data Portability**

1.64.1. Individuals will have the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:
1.64.1.1. the processing is based on consent or on a contract; and

1.64.1.2. the processing is carried out by automated means
1.64.1.3. this right is not the same as subject access and is intended to give individuals a subset of their data.

65. **The Right of Rectification and Restriction**

1.65.1. Individuals will have 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.

66. 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.

Marketing and Consent

67. The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing this will be done in a legally compliant manner.

68. The College will ensure that an individual's consent is a "clear affirmative action" through providing the means to opt in to future marketing.

69. The College will also abide by the Privacy & Electronic Communications Regulations when considering marketing or communicating by phone, email or text.

70. The College will only use a "soft opt in" approach to marketing where the following conditions are met:

1.70.1. contact details have been obtained in the course of sales or negotiations for a sale;
1.70.2. the College are marketing its own similar services; and
1.70.3. the College gives the individual a simple opportunity to opt out of marketing when first collecting the details and in every message after that.

71. Individuals who have paid the College membership fee may be contacted regarding similar courses and progression opportunities. In such cases the individual will be given the opportunity to opt out of any future correspondence.

Automated Decision Making and Profiling

72. Any Automated Decision Making or Profiling which the College may carry out will only take place once the College is confident that it is complying with Data Protection Laws. If College Personnel wish to carry out any Automated Decision Making or Profiling they must inform the Data Protection Officer.

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

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

Data Audit and Data Protection Impact Assessments

75. The College will regularly carry out a data audit of each of its' Schools and Departments.

76. This data audit process will form the basis of the College's Data Protection Impact Assessments (DPIA)and will:

    1.76.1. describe the collection and use of Personal Data;
    1.76.2. assess its necessity and its proportionality in relation to the purposes;
    1.76.3. assess the risks to the rights and freedoms of individuals; and
    1.76.4. the measures to address the risks.

77. The College will carry out a DPIA if launching or proposing to adopt a new process, product or service that uses Personal Data.

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

Transferring Personal Data Outside of the EAA

79. The College, in general, will not store or transfer Personal Data outside of Europe.

80. The College may transfer data outside the European Economic Area (EEA) in the process of using different marketing and email systems or through the use of third party service providers.

81. The College will only transfer Personal Data out of the EEA, where at least one of the following safeguards are in place:

    1.81.1. we will only transfer Personal Data to countries that the European Commission have approved as providing an adequate level of protection for Personal Data by; or
    1.81.2. where we use certain service providers, we may use specific contracts or codes of conduct or certification mechanisms approved by the European Commission which give Personal Data the same protection it has in Europe; or
    1.81.3. if we use US based providers that are part of EU-US Privacy Shield, we may transfer data to them, as they have equivalent safeguards in place.

82. If none of the above safeguards are available, the College may request your explicit consent to the specific transfer. You will have the right to withdraw this consent at any time.

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

Consequences of Failing to Comply

84. The College takes compliance with this policy very seriously. Failure to comply with the policy:

    1.84.1. puts at risk the individuals whose personal information is being processed; and
    1.84.2. carries the risk of significant civil and criminal sanctions for the individual and the College; and
    1.84.3. may, in some circumstances, amount to a criminal offence by the individual.

85. Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

86. If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer.

Appendix I: Definitions

The following definitions are based on the definitions contained in this Policy and the GDPR and include additional plain English explanations of various terms.

1.1. **College**: Capel Manor College

1.2. **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.

1.3. **Controller:** A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data that 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.

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

1.5. **Data Protection Officer:** Our Data Protection Officer is Richard Davies. If you have any questions about this policy or the ways in which we use your personal information, please contact our Data Protection Officer at: **dataprotection@capel.ac.uk**

1.6. **European Economic Area (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.

1.7. **ICO:** the Information Commissioner's Office, the UK's data protection regulator.

1.8. **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. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

1.9. **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 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.

1.10. **Processor:** Any 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 may be the 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.

1.11. **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.

1.12. **Automated Decision Making:** happens where a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects.

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