CAMBRIDGE REGIONAL COLLEGE
GREAT CAREERS START HERE

Data Protection Policy

Reference Number: EXA5

Version: 7

Page(s):	11
Approved SMT Date:	09/05/2018
Last Review Date:	20/07/2021
Review Frequency:	Annually
Next Review Date:	31/07/2022
Originator title:	Vice Principal Quality Improvement/Data Protection Officer
Author:	Vice Principal Quality Improvement/Data Protection Officer
Equality Impact Assessment Date:	Click here to enter a date.
Associated Policies:	• Privacy Notice • Storage and Retention of Personal Data and Administrative Documents Policy. • Staff Data Protection Guidance • Data Breach Procedure • Internet, Networking and Software Compliance Policy • Data Subject Access Policy

Aim

1. This document sets out the principles that Cambridge Regional College ('the College') will follow in relation to personal data that it processes. It also sets out staff obligations in relation to personal data.
2. The College is committed to protecting personal data about identifiable individuals both in private and professional capacities. As a business, the College needs to process personal data about students, employees, employers, clients and others.
3. This Policy is designed to:

- Outline the principles that determine the way that personal data will be held and handled by the College
- Ensure that employees are aware of their obligations in relation to personal data in their possession
- Explain how the College complies with the UK General Data Protection Regulations (UK GDPR) and Data Protection Act (2018).

4. This policy should be read in conjunction with the following key documents:
    i. Privacy Notice, which is on the College website and provides key information about the types of data processed, the reason for doing so, how long it is kept and the rights of individuals.
    ii. Storage and Retention of Personal Data and Administrative Documents Policy, which outlines the length of time different categories of data will be kept and arrangements for security and storage.
    iii. Data Subject Access Policy
    iv. Guidance for staff outlining good practice when processing personal data including use of technology to access data off site.
    v. Data Breach Procedure for staff
    vi. Internet, Networking and Software Compliance Policy

5. College Personnel will receive a copy of this Policy when they start and may receive 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.
6. More information on how to make a data access or amendment request can be found in Appendix 1.
7. More information on the definitions contained within the UK GDPR and used in this Policy is held within Appendix 2.

Principles

The College is committed to complying with the six principles of the General Data Protection Regulations, which came into force in May 2018:

1. Lawfulness, fairness and transparency
   The College will process personal data fairly and for a lawful purpose; we will publish clear, transparent and accessible information about the types of data we collect, the reason for doing so, how we keep it safely stored and for how long. We will include information about any third parties who process data on our behalf. We will publish this information in the College Privacy Notices. These can be found on the college website - https://www.camre.ac.uk/about/policies-reports/privacy-notice/
   If the college changes how it uses Personal Data, the College may need to identify Individuals about the change. If College Personnel therefore need to change how they use Personal Data they must notify the Data Protection Officer who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

2. Purpose limitation
   We will collect personal data for specified, explicit and legitimate purposes and we will not use it for unrelated purposes without notifying data subjects and where appropriate seeking informed consent.

3. Data minimisation
   We will collect the least amount of data required to carry out our stated purpose.

4. Accuracy
   We will take reasonable steps to ensure the data we collect and process is accurate and, where necessary, kept up to date. Depending on the purposes for which the data are processed, we will take every reasonable step to erase or rectify inaccurate data. 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).

5. Storage limitation
   We will keep data in a form which enables individuals to be identified for no longer than is necessary for the purpose for which the data are processed. We may archive personal data where this is in the public interest, scientific, or historical research purposes or statistical purposes; where we do this, we will ensure archived data is kept secure. We will outline how long we keep different categories of data in our Storage and Retention of Personal Data and Administrative Documents Policy.

6. Integrity and confidentiality
   We will keep personal data safe and protect it from unauthorised or unlawful use and against accidental loss, destruction or damage.

7. The College is committed to ensuring that the rights of data subjects (those individuals whose personal data we process) under GDPR are upheld. These are the rights to:
   i. Transparency
   ii. Subject access
   iii. Portability
   iv. Rectification
   v. Erasure
   vi. Restriction
   vii. Object to processing
   viii. Object to marketing
   ix. Object to automated decision making

8. We will publish clear guidance on how individuals can contact the College to request access to their data or to exercise other rights where these are available.

9. We will maintain an accurate record of data processing activities and will carry out Privacy Impact Assessments for new data processing activities.

10. We will only work with third party processors who can provide sufficient guarantees that the GDPR requirements will be met and the rights of data subjects protected.
11. We will not share personal data with third parties without appropriate data sharing agreements in place to ensure the principles of the GDPR are complied with.
    The College may share personal data in order to comply with legal or regulatory obligation, for example to provide information to the police carrying out an investigation or to OFSTED during an inspection. We will comply with GDPR principles and advise of new uses of personal data before we start using it for a new purpose.

11. The College processes sensitive personal data for the monitoring of equality and diversity. This information is used in analysis of statistical data. Data about health and disability is used to ensure that support for individual students and staff is in place. This data is subject to additional safeguards to keep it safe and secure, and to comply with GDPR and the DPA.

13. Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.
    a. Automated Decision Making happens where the College decides about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and
    b. Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.
    c. 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.
    d. College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.
    e. The College does not carry out Automated Decision Making or Profiling in relation to its employees.

14. Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and College Personnel must comply with the College's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which College Personnel need to comply with in the event of Personal Data breaches.

15. Personal Data breach is defined very broadly and is effectively any failure to keep 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.

16. There are three main types of Personal Data breach which are as follows:
    a. 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;
    b. 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

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

17. The College will provide training and guidance to staff in the principles of GDPR and the consequences of failing to comply with this legislation.

18. All College Personnel handling personal data are responsible for complying with the principles of GDPR and for keeping data safe and secure. All staff must comply with this policy and other guidance. Failure to do so may result in disciplinary action.

19. College Personnel must not release or disclose any Personal Data:
    a. outside the College; or
    b. inside the college to College Personnel not authorised to access the Personal Data,
    c. without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

20. 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.

21. The College retains the ownership of all data on college systems including emails. Details are set out in the Internet, Networking and Software Compliance Policy.

Appendix 1

Data Subject Rights

1. Data subject rights under UK GDPR are:
    i. Transparency
    ii. Subject access
    iii. Portability
    iv. Rectification
    v. Erasure
    vi. Restriction
    vii. Object to processing
    viii. Object to marketing
    ix. Object to automated decision making
2. Requests relating to data subject rights should be made in writing to the College Data Protection Officer who will acknowledge requests, and co-ordinate appropriate actions in line with UK GDPR, and this policy. A written response will be provided within 30 days where possible.
3. All requests for **data access** should be made in writing to the College Data Protection Officer
4. In certain cases, depending on the purpose for holding the data and the nature of the request we may be unable to comply, for example if personal data is needed by the College to comply with a legal obligation (for example sending payroll information to HMRC) or to perform a task carried out in the public interest. If this is the case we will inform the individual within 30 days of the request, explain why this is the case and how to contact the ICO (Information Commissioner's Office) to complain about this decision.
5. The College will respond within 30 days, unless the request is complex or a large amount of data is involved, in which case we may extend this timescale by up to a further 60 days. If we do this, we will advise the individual within 30 days of the request.
6. In light of the Covid-19 pandemic, our campuses may be subject to temporary closure. We will continue to meet our obligations in relation to Data Subject Access requests, however, it may be necessary to extend the 30 day response timeline. If this is the case, the College will write to you.
7. We will not usually charge for a data subject request but reserve the right to charge a reasonable administration fee for excessive or manifestly unfounded requests, if the request is repetitive. We may charge for request for further copies of the same information.

8. Requests for **data erasure or rectification**, i.e. to have inaccurate data rectified or completed if incomplete can be made verbally or in writing. Verbal or written requests can be made to appropriate members of the College staff, who are involved in processing data for example to teachers, tutors or assessors, members of the Student Administration or Curriculum Administration teams, exams officers, HR team. In most cases this will be acted upon quickly by the member of staff involved. Written requests can also be made directly to the College Data Protection Officer. All requests made directly to the DPO will be recorded, and written confirmation will be provided within thirty days.
9. Requests to **restrict or block processing** of personal data can be made in writing to the College Data Protection Officer. Where data processing is restricted the College will retain just enough personal information to ensure the restriction is respected. In some cases, the College's legitimate grounds for processing the data, for example if personal data is needed by the College to comply with a legal obligation (for example sending payroll information to HMRC) or to perform a task carried out in the public interest, and may override those of the individual.
10. When requested, personal data will be provided in a structured, machine-readable form to enable data to be used by other organisations. We will respond to such requests within 30 days, unless the request is complex or numerous, in which case we may extend this timescale by a further 60 days. If we are unable to comply with the request, we will respond within 30 days and include information about how to make a complaint to the ICO.
11. Requests to **object to processing** including direct marketing, processing based on legitimate interest or performance of a task in the public interest or for purposes of scientific/historical research and statistics can be made in writing to the College Data Protection Officer.
12. We will **stop processing personal data** for direct marketing purposes when we receive an objection. We will stop other processing unless we have legitimate grounds for processing which override the interests, rights and freedom of the individual. If this is the case we will advise the individual of this.
13. Requests in writing can be made to:

The Data Protection Officer
Cambridge Regional College
Kings Hedges Road
Cambridge CB4 2QT
or by email to DPO@camre.ac.uk

Appendix 2

Definitions

College - Cambridge Regional College

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.

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 UK 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 Corrin Hoyes and can be contacted at: DPO@camre.ac.uk or on 01223 226345

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.

Document history

Date	Issue number	Change/Comments	Date Approved	Approved by
21/04/2015	1	Document created	29/4/15	Head of MIS
09/01/2017	2	Annual Review – no changes made	9/1/2017	Head of MIS
1/5/2018	3	Significant revisions to prepare for GDPR	9/5/2018	DPO / SMT
20/5/2019	4	Annual Review – no changes made	20/05/2019	DPO
1/6/2020	5	Annual Review – amendment in relation to Covid-19 added para 18	01/06/2020	DPO
26/11/2020	6	DPA date updated to 2018	26/11/2020	DPO
20/07/2021	7	Amended to clarify appendix in relation to data subject rights; removed DSAR procedure to make this information more accessible. Added UK GDPR references.		DPO

CAMBRIDGE REGIONAL COLLEGE
GREAT CAREERS START HERE

Contact Us

enquiry@camre.ac.uk