

Data Subject Access Request Policy and Procedure

Reference Number: EXA06

Version: 8

Page(s):	12
Approved SMT Date:	08/07/2026
Last Review Date:	22/06/2026
Review Frequency:	Annually
Next Review Date:	31/07/2027
Originator title:	Head of Student Administration
Author:	Data Protection Officer
Equality Impact Assessment Date:	30/06/2025
Equality Impact Assessment Review Date:	31/07/2028
Associated Policies:	• EXA05 Data Protection Policy • COM4 Freedom of Information Act Policy

Overview

1. All individuals have rights over their personal data and Cambridge Regional College (the College) recognises the importance of having an effective policy in place to allow individuals to exercise those rights easily. This policy and procedure is in place to ensure that college staff are aware of the rights of each data subject, and the procedure to follow in the event of a data subject access or other data subject request being made.
2. It is our policy to direct significant requests for data access or amendment in line with UK GDPR data subject rights to the College Data Protection Officer who will co-ordinate a response and appropriate action.
3. College staff will receive regular training and updates relating to data protection.
4. This Policy does not form part of any College staff's contract of employment, and the College reserves the right to change this policy at any time. All College staff are obliged to comply with this policy at all times.

Scope

5. This policy applies to all College staff or other data processors who collect and/or use personal data relating to individuals.
6. It applies to all personal data stored electronically, in paper form, or otherwise.
7. Actions carried out by the Data Protection Officer may be delegated to the Assistant Data Protection Officer or other team member.

Definitions

8. **College** – Cambridge Regional College
9. **College Personnel** – Any College employee or contractor who has been authorised to access any of the College's personal data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.
10. **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.
11. **Data Protection Officer** – The Data Protection Officer is Corrin Hoyes and can be contacted at DPO@camre.ac.uk
12. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.
13. **Personal Data** – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.
14. **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.

Subject Access Request

College obligations

15. This Policy sets out the rights that individuals have over their personal data under Data Protection Laws. If a member of the College staff receives a request from an individual to exercise any of the rights set out in this policy, that member of the College staff must:
 - a. inform the Data Protection Officer as soon as possible and, in any event, within 24 hours of receiving the request
 - b. tell the Data Protection Officer what the request consists of, who has sent the request and provide the Data Protection Officer with a copy of the request
 - c. not make any attempt to deal with, or respond to, the request without authorisation from the Data Protection Officer or delegated person

Individual rights over personal data

Right of Access

16. Individuals have the right to ask the College to confirm the personal data about them that the College is holding, and to have copies of that personal data (commonly known as a **Subject Access Request, Data Subject Access Request, SAR or DSAR**. At College we use the term DSAR) along with the following information:
 - a. the purposes that the College has their personal data for
 - b. the categories of personal data about them that the College has
 - c. the recipients or categories of recipients that their personal data has been or will be disclosed to
 - d. how long the College will keep their personal data
 - e. 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);
 - f. 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
 - g. where the personal data was not collected from them, where the College got it from
 - h. the existence of automated decision-making, including profiling (if applicable).
17. 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 its administrative costs of making the further copy. The College can also charge a reasonable fee if it considers the request to be excessive, for example repetitive or vexatious.

18. There are no formality requirements to making a DSAR and it does not have to refer to data protection law, or use the words Subject Access Request or SAR.
19. The College is required to respond to a DSAR within one calendar month from the date the College receives it and has sufficient information to start processing the request (including confirming the identity of the person making the request). If the DSAR is complex or there are multiple requests at once, the College may extend this period by a further two months provided that the College tells the individual who has made the DSAR about the delay and the College's reasons for the delay within the first calendar month.
20. The Data Protection Officer will reach a decision as to the complexity of the DSAR and whether the College is entitled to extend the deadline for responding.

Right to rectification

21. 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 calendar month (or a further two months if the request is complex).
22. 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.
23. 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.
24. 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 calendar month of them making the request

Right to erasure (right to be forgotten)

25. Individuals have the right to ask the College to delete the personal data the College has about them in certain circumstances, but this right is limited in scope and does not apply to every individual. The right to be forgotten applies when:
 - i. the personal data is no longer necessary for the purpose the College collected it for
 - j. the individual withdraws consent and the College has no other legal basis to use their personal data
 - k. the individual objects to the College's processing and there is no overriding legitimate interest for continuing the processing
 - l. the personal data was unlawfully processed
 - m. and/or the personal data has to be erased to comply with a legal obligation.
26. 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.
27. 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 calendar month of them making the request that this has been done.

Right to restrict processing

28. Individuals have the right to “block” or “suppress” the College’s processing of their personal data when:
 - a. they contest the accuracy of the personal data, for a period enabling the
 - b. College to verify the accuracy of the personal data;
 - c. the processing is unlawful and the individual opposes the deletion of the personal data and requests restriction instead;
 - d. 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;
 - e. 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
29. 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.
30. 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 calendar month of them making the request that this has been done.

Right to data portability

31. 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.
32. The right to data portability only applies when
 - a. the individual provided the College with the personal data;
 - b. the processing the College is carrying out is based on the individual’s
 - c. consent or is necessary for the performance of a contract; and
 - d. the processing is carried out by automated means.
33. 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.
34. The College is obliged to provide this information free of charge within one calendar month of the individual making the request (or a further two months where the request is complex provided that the College explains to the individual why it needs more time).
35. The individual also has the right to ask the College to transmit the personal data directly to another organisation if this is technically possible.

Right to object

36. Individuals have the right to object to the College’s processing of their personal data where:

- a. 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 their particular situation on which to object
 - b. the College is carrying out direct marketing to the individual; and/or
 - c. the College's processing is for the purpose of scientific/historical research and statistics and the individual has grounds relating to their particular situation on which to object.
37. 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.
38. 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.
39. Before the end of calendar 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

40. Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is:
- a. necessary for entering into or performing a contract between the College and the individual
 - b. required or authorised by Data Protection Laws
 - c. based on the individual's explicit consent.
41. **Automated decision making** happens where an organisation makes a decision about an individual solely by automated means without any human involvement; **Profiling** happens where an organisation automatically uses personal data to evaluate certain things about an individual.

Data Subject Rights Procedure

If a member of college staff receives a request from an individual to access or to receive a copy of their personal data, or for it to be rectified or erased the following procedure will be followed:

The college staff member must forward or report the request to the Data Protection Officer as soon as they receive it.

1. A request from an individual does not have to be in a particular format, for example it does not have to be in writing. If the request is not made in writing (e.g. it is taken over the telephone) best practice is that the college asks the individual to confirm in writing so it can ensure it is complying correctly with the request. If they do not wish to do this, then please confirm the request in writing and ask them to indicate if there are any inaccuracies.
2. The college will not charge a fee for responding to these requests unless a second or subsequent copy of personal data is requested (in which case the college can charge its administrative costs) or the request is unfounded or excessive.
3. The Data Protection Officer will diarise the date the request was received, the deadline to respond, (ordinarily one calendar month from the date of receipt) but an extension may be possible in certain circumstances. The Data Protection Officer will send reminders to all college staff involved in dealing with the request in order to track its progress
4. Within 2 working days of receipt, the Data Protection Officer will decide whether any further information is needed from the individual to clarify the identity of the individual or to understand the request and will ask the individual for any further information that is needed as soon as possible; if further information is required, no action will be taken until the further information has been received from the individual
5. Once the further information has been received and/or the college is satisfied that it knows what has been asked for, the college will begin locating the individual's personal data
6. Depending on who the individual is, this may involve locating staff files, student files, information on parents, notes, minutes, correspondence and other relevant documents containing personal data either on the college's information systems, or in the college's structured paper filing systems. The Data Protection Officer will let college staff know what searches they need to carry out
7. Once the college has conducted a reasonable search for all the personal data of the individual, the following will apply:

Data Subject Access:

8. Data Protection Officer will review it and decide whether any of the personal data does not need to be disclosed as there are exemptions which may apply
9. Data will be redacted to remove third party personal information, for example the names of other students or members of staff
10. Once the college has decided what the college is going to provide to the individual, the college will respond providing copies of the personal data, which, if the request is made electronically, shall be provided in a commonly used electronic form
11. If the college fails to do this within one calendar month of the date the college receives the request, the college will ensure that it has contacted the individual before the deadline

to explain what the college has done so far and when the college will get back to them with their personal data.

Right to rectification:

12. The College will then locate the personal data concerned and verify whether it is incorrect or incomplete and will correct it or complete it as soon as possible
13. The College will ascertain whether the College has disclosed the incorrect personal data to any third parties and, if so, the College will contact those third parties as soon as possible to tell them to correct the personal data
14. The Data Protection Officer will decide whether the College needs to keep a copy of the original personal data for evidence reasons or otherwise; and
15. The College will confirm to the individual in writing within one calendar month of the date of their request that the College has complied with the request.

Right to erasure:

16. The Data Protection Officer will reach a decision as to whether the right to be forgotten applies;
17. If the right to be forgotten does apply, the Data Protection Officer will decide whether the College is required to keep any parts of the personal data for evidence reasons and, if so, this personal data will be excluded from the request
18. The College will then securely delete all the personal data about that individual that the College has which is not excluded. This will include securely shredding all hard copy documents and ensuring that computer records are securely deleted from the College's information systems in line with the processes detailed in the College's Data Retention Policy.
19. The College will ascertain whether it has disclosed the deleted personal data to any third parties and, if so, the College will contact those third parties as soon as possible to tell them to delete the personal data; and
20. The College will confirm to the individual in writing within one calendar month of the date of their request that the College has complied with the request.

Right to restrict processing

21. If a member of the College receives a request from an individual to restrict the College's use of their personal data, the following procedure will be followed:
22. The staff member must forward or report the request to the Data Protection Officer as soon as they receive it;
23. The Data Protection Officer will diarise the date the request was received, the deadline to respond and send reminders to all staff involved in dealing with the request in order to track its progress;
24. The Data Protection Officer will reach a decision as to whether the right to restrict processing applies
25. If the right to restrict processing does apply, the College will action the request as soon as possible and ensure that the College no longer uses the individual's personal data in the way they have objected to. This may include moving documents to folders where they can no longer be accessed, removing details from files and locking paper files away

26. The College will ascertain whether the College has disclosed the Personal Data to any third parties and, if so, the College will contact those third parties as soon as possible to tell them to stop using the personal data in the restricted way;
27. The College will confirm to the individual in writing within one calendar month of the date of their request that the College has complied with the request.

Right to data portability

28. All requests for data access to be provided in a machine readable format will be complied with where possible; it is our policy to provide electronic copies of subject access data to all, as most of our processing is in this format.

Right to object

29. If a member of the College receives an objection from an individual to the College's processing of their personal data, the following procedure will be followed:
30. The staff member must forward or report the request to the Data Protection Officer as soon as they receive it
31. The Data Protection Officer will diarise the date the request was received, the deadline to respond, and send reminders to all College Personnel involved in dealing with the request in order to track its progress
32. The Data Protection Officer will reach a decision as to whether the right to object applies
33. If the right to object does apply, the College will action the request as soon as possible. This may include suppressing the individual from the College's direct marketing lists, or stopping the processing of Personal Data that has been objected to; and
34. The College will write to the individual within one calendar month of the date of their request to tell them either that the College has complied with, or intends to comply with, their request or that the College has not complied and the reasons why the College has not complied.

Rights in relation to automated decision making

35. If a member of the College receives an objection from an individual to an automated decision that the College has made about the individual which produces legal effects concerning them or similarly significantly affects them, the following procedure will be followed:
36. The staff member must forward or report the request to the Data Protection Officer as soon as they receive it;
37. The Data Protection Officer will diarise the date the request was received, the deadline to respond and send reminders to all College Personnel involved in dealing with the request in order to track its progress;
38. The Data Protection Officer will reach a decision as to whether the right to intervene in the automated decision-making applies
39. If the right to intervene does apply, the College will action the request as soon as possible. This will involve reviewing the automated decision-making process, reviewing the decision that was made, having a College Personnel consider whether the decision needs to be retaken and allowing the individual to give their view on the decision; and

- 40. The College will write to the individual within one calendar month of the date of their request to tell them what the outcome of the College's review is.
- 41. Automated decision making happens where the College makes a decision about an individual solely by automated means without any human involvement; and
- 42. Profiling happens where the College automatically uses personal data to evaluate certain things about an individual.

Are there any requests the College does not have to respond to?

- 43. If the request the College receives from an individual is unfounded or excessive then the College may either:
 - a. Refuse to action the request; or
 - b. Charge a reasonable fee taking into consideration the College's administrative costs of providing the information or taking the action requested.
- 44. Any decisions in relation to not actioning the request or charging a fee shall be made by the Data Protection Officer.

Response Times

- 45. All requests set out above must be responded to within one calendar month unless the request is complex in which case the period may be extended up to a further two months. Any decision in relation to whether the request is complex is to be made by the Data Protection Officer who shall inform the individual making the request of the extension. Any notification of the extension to the individual shall be made within the initial one-month period and shall give reasons for the delay.
- 46. If the College is not going to action the request made by an individual, the Data Protection Officer shall communicate this to them within month of receipt of the request. The communication shall include details of the College's reasons for not actioning the request and the ability of the individual to make a complaint.

Complaints

- 47. If an individual is dissatisfied with the way the College has handled a Data Subject Request, they should raise their concerns with the Data Protection Officer in the first instance at **DPO@camre.ac.uk**
- 48. The College will investigate the complaint and respond within 30 days. Where appropriate, the College will explain the reasons for any decision made.
- 49. If the individual remains dissatisfied following the College's response, they have the right to lodge a complaint with the Information Commissioner's Office (ICO).

Legal Advice

- 50. Specialist external legal advice may be taken on the above, but this shall be the decision of the Data Protection Officer or other member of the Senior Management Team

Document history

Date	Issue number	Change/Comments	Date Approved	Approved by
21/04/2015	1	Document created	29/04/2015	Head of MIS
09/01/2017	2	Annual Review – no changes made	09/01/2017	Head of MIS
21/05/2018	3	Document substantially changed to reflect GDPR	21/05/2018	DPO
10/01/2020	3	Annual Review – no changes		DPO
22/07/2022	4	Merged policy and procedure into one document to reduce excess documentation; renamed document		DPO
28/07/2023	5	Annual review – no change	28/07/2023	DPO
31/07/2024	6	Annual review – no change	31/07/2024	DPO
31/07/2025	7	Annual review – some changes to format to support readability. Added line 7 in the policy clarifying delegation to the Assistant DPO	31/07/2025	DPO
22/06/2026	8	Annual review – updated timescales from 30 days to one calendar month. Added complaints section (sections 47–49) to reflect current data protection legislation and ICO guidance.	08/07/2026	DPO

