

# Data Protection Policy



<b>OWNED BY:</b>		<b>Vice Principal Curriculum &amp; Quality</b>					
<b>DATE OF LAST REVIEW</b>		<b>October 2023</b>					
<b>PLANNED NEXT REVIEW:</b>		<b>October 2025</b>					
<b>APPROVAL:</b>		<b>Corporation</b>					
<b>APPLIES TO:</b>	Staff	Y	Students	Y	Public	N	

## 1. Policy Statement

1.1.1 The purpose of the DPA (Data Protection Act) 2018 is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent. This was previously the Data Protection Act 1998, which was replaced with the current act in 2018 with the introduction of the GDPR (General Data Protection Regulation) which while not altering the basic requirements of the DPA 1998 does require greater definition and clarity on most aspects. For example, the reasons for holding and processing data are now much more explicit and retention periods have to be clearer.

The GDPR came into law in May 2018 and the College has interpreted requirements based on official guidance, for example from the Information Commissioner's Office, experience of other Colleges as well as other relevant sources. We expect the working of the regulation to alter over time and this policy will be updated to reflect this. Staff, students or other parties requiring clarification on any GDPR related issue should contact the Data Protection Lead or Deputy Data Protection Lead.

1.1.2 Cirencester College needs to keep certain information about staff, students and other users to allow it to monitor, for example, performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College complies with the Data Protection Principles set out in the Data Protection Act 2018 ("the Act") and the GDPR. In summary these state that personal data shall:

- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up-to-date.
- Not be kept longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the United Kingdom unless that country has equivalent levels of protection for personal data.

1.1.3 The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. The policy applies to all staff and students of the College. Any breach of the Act or the College Data Protection Policy is considered to be an offence and in that event Cirencester College disciplinary procedures will apply.

- 1.1.4 It is a requirement of the GDPR that before other agencies and individuals working with the College can have access to personal information they have to sign a processing agreement with the College. The exception to this is safeguarding – where it is in the best interest of the child as defined by Keeping Children Safe in Education. Such an agreement will detail; the information being passed, the purpose that information is being passed for, the duration it will be held, and whether it will be passed to any other party.
- 1.1.5 All departments and sections who deal with external agencies will ensure that a suitable processing agreement is in place and has been approved by the Data Protection Lead.
- 1.1.6 The College Data Protection Lead is the VP Curriculum & Quality and the College Data Protection Deputy Lead is the MIS Manager with admin support provided by the College Quality Administrator.

## 2. Definitions

- 2.1.1 **Data Breach:** is when data, either hard or soft copy, are disclosed to a person or an organisation that it should not have been. That is, where there is no formal agreement to disclose information.
- 2.1.2 **Personal Data:** Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, and telephone number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.
- 2.1.3 **Sensitive Data:** Different from ordinary personal data (such as name, address, telephone) and relates to sexuality, racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.
- 2.1.4 **Data Controller:** Any person (or organisation) that makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed. Under the GDPR the College is the Data Controller for almost all data it holds.
- 2.1.5 **Data Subject:** Any living individual who is the subject of personal data held by an organisation.
- 2.1.6 **Processing:** Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data, accessing, altering, adding to, merging, or deleting data. Retrieval, consultation or use of data disclosure or otherwise making available of data.
- 2.1.7 **Third Party:** Any individual or organisation other than the data subject, the data controller (College) or its agents.
- 2.1.8 **Requestor:** Any person who has a personal interest in exercising the right to a Subject Access request.
- 2.1.9 **Source:** A recognised and lawful source of personal data collection.
- 2.1.10 **Disclosure:** A recognised and lawful recipient of personal data (in compliance with the purpose of processing).
- 2.1.11 **Unauthorised:** Any third party that receives data without the Colleges authorisation.
- 2.1.12 **Relevant Filing System:** Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails),

paper-based, photographic etc. from which the individual's information can be readily extracted.

**2.1.13 Data:** Information which is:

- Being processed by means of equipment operating automatically in response to instructions given for that purpose.
- Recorded with the intention that it should be processed by means of such equipment.
- Recorded as part of a relevant filing system (a structured system).
- Part of an accessible record. This includes such things as manual index card files, microfiche, etc.

### 3. Responsibilities

3.1.1 The College as a corporate body is the Data Controller under the Act.

3.1.2 The Data Protection Lead is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for members of the College.

3.1.3 The College Leadership Team, Faculty Heads, Section Heads and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the College.

### 4. Status of the Policy

4.1.1 This policy does not form part of the contract of employment but it is a condition of employment that staff will abide by the rules and policies made by the College. Any failure to follow the policy can therefore result in disciplinary proceedings. In certain serious circumstances such as (but not exclusively) unauthorised disclosure of information, this may constitute gross misconduct and could result in dismissal.

4.1.2 Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Protection Lead initially. If the matter is not resolved it should be raised as a formal grievance.

### 5. Privacy notices

5.1.1 The College has three privacy statements that are used to reflect the general approach to data retention, processing and management; one for students, one for staff and one for parents, carers and guardians. These statements are inserted into relevant processes and procedures, or referred to in those documents.

#### 5.2 Student privacy statement

5.2.1 While you study with us, the College will hold information relevant to your learning as well as physical and emotional support, we will not hold anything that is not for the express aim of supporting you. Part of this requires the College to pass information to other companies, such as our online shop, as well as Government agencies such as the Department for Education. In some circumstances we will pass contact information in support of government initiatives, in such cases you will then have an option to opt in to the service. There are also situations where another institution has a legal duty to provide information that we hold, for example your local authorities have to report to the Government where you went after leaving school, we will share such information but we will restrict it to the bare minimum, make it very clear why we are sharing it and limit what it can be used for. Two years after you would have left the College, where technology allows, we will anonymise or delete the information we hold other than core things such as your name, the programme you studied and the grades you got which we will hold for up

to seven years after you leave. Therefore, processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. There is a full list of the information we hold, why we hold it, how long we hold it for and who we pass it to available on the student zone.

### 5.3 Staff privacy statement

- 5.3.1 When managing an employee's personal data, information will be collected in accordance with the College's data protection policy. Data collected is held securely and accessed by, and disclosed to, individuals only for the purposes of information relating to this policy. Inappropriate access or disclosure of employee data constitutes a data breach and should be reported in accordance with the organisation's data protection policy immediately. It may also constitute a disciplinary offence, which will be dealt with under the College's disciplinary procedure.

### 5.4 Parent, carer, guardian privacy statement

- 5.4.1 The College holds contact details (email, land line phone number, mobile phone number and postal address) so that we can share information with parents, carers and guardians on such things as the progress of students, for example attendance, and for events such as parents evening. These details will be held securely for two years after the student would have left the College. The College will not disclose these details to any third party. Most members of staff will have access to contact details but it is expressly against the College Data Protection Policy and Staff Code of Conduct for this to be used for anything other than College business.

## 6. Notification of Data Held and Processed

- 6.1.1 Notification is the responsibility of the Data Protection Lead.

- 6.1.2 All staff, students and other users are entitled to:

- Know what information the College holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up-to-date.
- Know what the College is doing to comply with its obligations under the Act.

## 7. Responsibilities of Staff

- 7.1.1 All staff are responsible for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information, which they have provided, e.g. changes of address.
- Checking the information that the College will send out from time to time, giving details of information kept and processed about staff.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

- 7.1.2 Compliance with data protection legislation is the responsibility of all members of the College who process personal information. Members of the College are responsible for ensuring that any personal data supplied to the College are accurate and up-to-date.

- 7.1.3 Employees are responsible for ensuring that confidential information is kept in a secure place. In addition, staff must only keep information, either soft copy on computers or hard copies in storage, which is directly related to the learning of the student or the emotional and physical

support of a student.

7.1.4 Such information should be removed, or anonymised, when the student leaves the College; and must be deleted, or anonymised, no longer than twenty-four months after they would have left except where legislation requires that details are kept for longer.

7.1.5 In particular staff must take the following approach to the storing of such data, on both computer system and hard copies in drawers and filing cabinets:

- Delete data on ex-students when they leave where this is easy to do so.
- If staff come across any data on past students, delete it.
- Store information with a view to easy deletion as students depart.

## 8. Data Protection Principles

8.1.1 All processing of personal data must be carried out in accordance with the eight data protection principles.

- 1) Personal data shall be processed fairly and lawfully. This means that the College will only hold and process data where there is a clear need in order to support the learning and emotional needs of students, or the employment of staff. The College will provide details of the data held and the purpose for holding it.
- 2) Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes. Data obtained for specified purposes must not be used for a purpose that differs from those.
- 3) Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held. Information, which is not strictly necessary for the purpose for which it is obtained, will not be collected. If data are given or obtained which is excessive for the purpose, they will be deleted or destroyed.
- 4) Personal data shall be accurate and, where necessary, kept up to date. Data, which are kept for a long time, will be reviewed and updated as necessary. No data will be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the College are accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate. Individuals must notify the College of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the College to ensure that any notification regarding change of circumstances is noted and acted upon.
- 5) Personal data shall be kept only for as long as necessary. The College will detail how long it will hold and process data for. Where it is technically possible data exceeding these dates will be deleted or anonymised such that a data subject cannot be identified. Any information that exceeds these dates but which cannot be deleted or suitably anonymised will be secured and not disclosed.
- 6) Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act and the GDPR.
- 7) Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.
- 8) Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory is GDPR compliant.

## 9. Data Subject Rights

9.1.1 Data Subjects have the following rights regarding data processing, and the data that are

recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of an automated decision-making process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

## 10. Student Obligations

10.1.1 Students must ensure that all personal data provided to the College are accurate and up to date. They must ensure that changes of address are notified to the Student Journey.

10.1.2 Students who use the College computer facilities may, from time to time, process personal data. If they do they must notify the designated Data Protection Lead or Deputy. Any student who requires further clarification about this should contact the designated Data Protection Lead or Deputy

## 11. Data Security

11.1.1 All members of staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.

11.1.2 All personal data should be accessible only to those who need to use it. You should form a judgment based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access.
- In a locked drawer or filing cabinet.
- If computerised, password protected.

11.1.3 Care should be taken to ensure that PC monitors are not visible except to authorised staff and that computer passwords are kept confidential. PC monitors should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel. Offices should be locked when unattended.

11.1.4 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs must be wiped clean before disposal or as part of a certified process.

11.1.5 This policy also applies to staff and students who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside the College Campus.

11.1.6 The College does not want to stop staff working at home, but we do want to make sure that they do so securely. Be very aware that anyone other than a member of staff, or authorised external party, seeing any data on staff or students is considered a data breach

#### 11.1.7 The following guidelines should be followed:

- Work in an area that is private from other members of the household.
- Lock hard copies away when not being worked on.
- By preference do not copy data to personal PCs, use OneDrive where possible.
- Only keep data on personal PCs for the time that is needed making sure to fully delete, i.e. empty the Recycle or Trash bin.
- For full deletion use tools such as CCleaner or Eraser.
- Only keep hard copies at home for the duration actually needed for the task being undertaken, then either return to College or destroy.
- Do not use a desktop PC for access to College email, use the Outlook Web App.
- By preference do not use USB memory sticks to transfer files instead use OneDrive.
- If using a USB memory stick ensure that it is password protected.
- When you have finished with a PC, for example upgrading or passing to someone else, make sure that all data is destroyed.

11.1.8 Some staff also connect to College email on their phone. This means that emails, and potentially attachments, are held on the phone. There is some risk of others seeing those emails but as phones are personal the risk is low. The main concern is when a phone is lost or sold. When selling, or passing on, a phone a “reset to factory settings”, or equivalent, should always be done. But when lost this can’t be done automatically. There are apps available to install on phones that mean when triggered a “reset to factory settings” is forced, which staff are encouraged to install. Phones should be locked with a pin code or biometric passkey such as fingerprint or iris scanner.

## 12. [Rights to Access Information](#)

**See Appendix A for Subject Access Data Form**

**See Appendix B for What other information an individual is entitled to**

12.1.1 Staff, students and other users of the College have the right to access any personal data that are being kept about them either on computer or in certain files. Some data will not be provided, such as references marked as confidential, that are exempt under UK GDPR law.

12.1.2 Any Requestor should write formally to the College and must complete the above form, giving details of the information they require and provide identification such that their identity, and therefore their legal rights, can be confirmed. The College may secure the assistance of authorised 3rd parties to support prompt and accurate compliance with the SAR, in which case a full Confidentiality, Data Sharing and Data Processing agreements will be signed by the Colleges DPL and the data checking company. Appropriate due diligence will be carried out prior to authorised appointments.

12.1.3 The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month unless there is good reason for delay and in which case the one-month period would be extended to three months. In such cases, the reason for delay will be explained in writing to the data subject making the request. In any event the one-month period will not start until the College has received the SAR form including:

- all information reasonably required to identify the data subject;
- proof of identity
- Reasons for the request
- Signed consent



12.1.4 Any inaccuracies in data disclosed in this way should be communicated immediately to the Data Protection Lead who will take appropriate steps to make the necessary amendments.

**Under the act, the College can refuse a request if it is manifestly unfounded or manifestly excessive and the requestor will be informed at the earliest opportunity.**

## 13. Disclosure of Data

13.1.1 The College must ensure that personal data are not disclosed to unauthorised third parties. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter.

13.1.2 No employee must divulge any personal information on students, current or former, or members of staff unless the employee has explicit authorisation to do so.

13.1.3 Personal information for students includes, but is not limited to; addresses, email addresses, attendance, grades, and issues with health, safeguarding or academic support. For staff; contact details, employment history, sickness and disciplinary details.

13.1.4 Staff must give particular consideration when forwarding emails to ensure that personal details are not disclosed which includes when carbon copying recipients on emails when care must be taken not to disclose email address inappropriately.

13.1.5 Only designated people can issue references on behalf of the College either as part of a formal process, for example UCAS, or less formally, for example to agencies, employers or other educational institutions. Generally, those with this designation are confined to HR and Student Journey. If staff wish to provide personal references they must not be done from a College email account, or be on College headed paper, and must be clear that they are not being sent on behalf of the College.

13.1.6 For those with the appropriate designation data may be legitimately disclosed where one of the following conditions applies:

- The individual has given their consent (e.g. a student/member of staff has consented to the College corresponding with a named third party).
- Where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other College employees if it is clear that those members of staff require the information to enable them to perform their jobs).
- Where the institution is legally obliged to disclose the data (e.g. ESFA, ethnic minority and disability monitoring).
- Where disclosure of data is required for the performance of a contract.

13.1.7 The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security\*;
- prevention or detection of crime including the apprehension or prosecution of offenders\*;
- assessment or collection of tax duty\*;
- discharge of regulatory functions (includes health, safety and welfare of persons at work\*);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.



\* Requests must be supported by appropriate paperwork, for example Court Orders.

13.1.8 When members of staff receive enquiries as to whether a named individual is a member of the College, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed the member of staff should decline to comment. Even confirming whether or not an individual is a member of the College may constitute an unauthorised disclosure.

13.1.9 Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

13.1.10 As an alternative to disclosing personal data, the College may offer to do one of the following:

- pass a message to the data subject asking them to contact the enquirer;
- accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

13.1.11 Please remember to inform the enquirer that such action will be taken conditionally, i.e. "if the person is a member of the College" to avoid confirming their membership of, their presence in or their absence from the institution.

13.1.12 If in doubt, staff should seek advice from their Faculty Head /Section or the College Data Protection Lead.

## 14. Data breaches

14.1.1 If a member of staff, student, family member, visitor or member of the public believes that there has been a data breach this must be reported to the College Data Protection Lead and the data breach form must be completed on CCO too. Near misses must also be recorded on the data breach near miss form on CCO

14.1.2 The DPL will provide guidance on whether there has been a breach, and any action that needs to be taken.

14.1.3 If the breach meets the relevant guidelines of the Information Commissioner's Office a full report will be provided by the DPL, subject to the ICO requirements, within the legal target of 72 working hours

14.1.4 The DPL will issue, via the SLT, instructions on any changes in practice.

14.1.5 Any requirement to invoke disciplinary procedures will be discussed with the Head of HR and if required the appropriate policy followed.

## 15. Publications of College Information

15.1.1 It is College policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Information on examination results.
- Information in prospectuses (including photographs), annual reports, staff newsletters, etc.

15.1.2 The College's internal phone list will not be a public document.

15.1.3 Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Protection Lead.

15.1.4 It is recognised that there might be occasions when a member of staff, a student, or a lay member of the College, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the College should comply with the request and ensure that appropriate action is taken.

## 16. Processing Sensitive Information

16.1.1 Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. The College will not need such consent if processing is necessary for a) complying with a legal obligation imposed on the College, b) to keep an Equal Opportunity Policy under review where the data is about race or ethnic origin, or c) (in emergencies) protecting the data subject or a third party who cannot give consent.

16.1.2 Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students may be asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Data Controller.

16.1.3 If an employee considers that the College holds information which is likely to cause damage or distress to that individual, the employee has the right to write to the College requesting the deletion of the information. If the employee has previously consented to that information being held, the College may decide not to comply with the request or if the information is necessary for contractual or legal reasons or to protect the organisation's vital interests.

## 17. Retention of Data

17.1.1 As a general principle the College will only keep information for as long as it is legitimately required. General principles are:

- Student study data: the majority of information for two years after they would have completed studies if they had attended for the full term. High level information, i.e. courses studied and grades achieved for as long as the ESFA (Education and Skills Funding Agency) requires, which is currently six years plus the current one.
- Application data: until the student enrolls or for one year after the date that they would have enrolled.
- Staff data: core information, i.e. period employed and role undertaken, wages earned, for up to seven years after departure.
- Where staff and students have applied to the college but the application has not been processed for whatever reason, the data will be removed with immediate effect.

17.1.2 Any former employee who does not wish the College to retain such information for this period should write to the Head of Human Resources and request that their file is securely disposed of.

## 18. Marketing and publicity

18.1.1 Any department or section that uses personal data for marketing or publicity purposes must obtain consent from data subjects of this at the time of collection of the data, which includes photos. Individuals must be provided with details of how the data will be used and the time period before giving written, or email, consent. This includes all publicity information including

posters used within the College, social media and formal publications.

18.1.2 As a part of its normal post exam and end of course processes the College will use positive examples of success in carefully targeted advertising, for example on banners when visiting prospective students in schools and on open days and for selected press releases. The College assumes implied consent to do this when students enrol, if students do not wish their results to be included they must contact the Student Journey.

## 19. Use of CCTV


19.1.1 For reasons of personal security and to protect College premises as well as the property of staff and students, close circuit television cameras are in operation in certain campus locations. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out only by a limited number of specified staff.
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete.
- Staff involved in monitoring will maintain confidentiality in respect of personal data.
- Recordings are kept only for four days unless there is a serious incident being investigated in which case recordings will be kept for two weeks.

## 20. Conclusions

20.1.1 Compliance with the Act and with the GDPR is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the College Data Protection Lead.

## Appendix A

 <b>cirencester college</b> <small>a beacon college</small>	<b>Data Protection Act 2018</b>  <b>Subject Access Request Form</b>
--	---

We need the following information to help us to give you a quick and accurate response to your request. Please note the information requested will be delayed if a suitable form of identification is not provided. Please provide the information required below and return it to:

**The Data Protection Lead**  
**Cirencester College**  
**Stroud Road Cirencester**  
**GL7 1XA**

### Part A - Your Details

<b>Title</b>	
<b>Surname</b>	
<b>Forename(s)</b>	
<b>Address</b>	
<b>Contact Telephone number(s)</b>	
<b>Contact e-mail address</b>	
<b>Relationship to Cirencester College</b>	
<b>Staff/student number</b>	
<b>Please say why you have requested this data?</b>	
<b>Please be as specific as possible about the data you want and the dates involved so that we can get it for you as swiftly as possible</b>	<b>Dates: --/--/---- to --/--/----</b>
<b>Does this include emails you have sent?</b> <b>Does this include emails you have been copied into?</b> Please note that either of these could delay your request because of the volume of work required	<b>Yes/No</b>  <b>Yes/No</b>
<b>Description of your request (What data do you want exactly?)</b> Please add any information which will enable us to locate your personal data e.g. emails between persons A & B; HR records; specific subject(s) or date(s).	
<b>I would like to receive this information in the following format: e.g. Email;</b>	
<b>Date of request</b>	
<b>Official use: date request received</b>	

**Part B – Proof of identity**

The Data Protection Act requires the College to satisfy itself as to the identity of the person making the request. The Data Protection Lead will need to see a relevant form of identification including a photograph. This may be the College's staff/student card, passport or driving licence. If it is problematic to supply this documentation please contact us to discuss alternative proof of identity arrangements. If the College is unable to satisfy itself as to your true identity from the documentation provided, we will contact you as soon as possible.

**Part C – Declaration**

I am the Data Subject named in Part A of this document, and hereby request, under the provisions of Section 7(1) of the Data Protection Act 2018, that Cirencester College provide me with copies of my personal data as requested and described in Part A.

**Signed:****Date:**

## Appendix B

### What other information is an individual entitled to?

Individuals have the right to receive the following information (which largely corresponds with the information that you should provide in a privacy notice):

- your purposes for processing;
- categories of personal data you're processing;
- recipients or categories of recipient you have or will be disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);
- your retention period for storing the personal data or, where this is not possible, the criteria for determining how long you will store it;
- the individual's right to request rectification, erasure or restriction or to object to processing;
- the individual's right to lodge a complaint with the Information Commissioner's Office (ICO);
- information about the source of the data, if you did not obtain it directly from the individual;
- whether or not you use automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual; and
- the safeguards you have provided where personal data has or will be transferred to a third country or international organisation.