**DATA PROTECTION POLICY v7.0**

**Table of Contents**

## 1. Revision History

| Version | Date | Author | Summary of changes |
|---|---|---|---|
| 7.0 | February 2025 | Michael Kemp | • Added 'Table of Contents' for easier navigation.<br>• Changed all references of Data Protection Officer to Information Governance Manager where appropriate.<br>• Added clause outlining information governance management framework and roles.<br>• Added a requirement for all staff to report subject access requests within one working day.<br>• Removed outdated reference the Schrems II case.<br>• Added section outlining requirement to centrally log and periodically 'refresh' data subject's consent.<br>• Added new Artificial Intelligence section.<br>• Removed outdated references to IT security and Social Networking policies.<br>• Expanded on auditing clause to further clarify how compliance will be monitored.<br>• Removed or changed some sentences throughout for brevity or increased reader clarity. |

## 2. Introduction

2.1. This policy deals with the appropriate acquisition, storage, processing, sharing and disposal of personal data by the Chichester College Group. From now on in this document references to the Chichester College Group will be simplified to the "Group". In scope are all people, information, technologies, resources and facilities that deal with information relating to an identifiable person who can be directly or indirectly identified.

2.2. This policy will not form part of the formal contract of employment, but it is a condition of employment that members of staff will abide by the rules and policies made by the Group. Any failure to follow this policy can result in disciplinary proceedings.

2.3. Any member of staff who considers that the policy has not been followed in respect of the data held about them should raise the matter with the Information Governance Manager. If they have concerns, they can also refer to the Information Commissioner's Office Website for further guidance.

2.4. The Group has to collect data about its members of staff, students, clients and other users to allow it to monitor performance, achievements, health and safety and security. It is also necessary to process this data so that staff can be paid, courses organised and legal obligations to funding bodies and government complied with.

2.5. Data also enters the public domain through social networking sites and emails. Therefore, the security of data transferred via these methods is also subject to the data protection principles.

2.6. In managing data on a day-to-day basis, the Group will adhere to the data protection principles prescribed by current Data Protection legislation and associated regulations.

2.7. It is a requirement that the Group is both responsible for and can demonstrate compliance with the data protection principles detailed in section 3.1 below, as

well as with the principles, rights and requirements for processing personal data in section 3 below.

## 3. Principles, Rights and Requirements for Processing Personal Data

3.1. The term "processing" in this context is the same definition as Article 4(2) of the UK GDPR.

3.2. The Group must have a valid lawful basis for processing personal data. These are:

- Fulfilment of contractual obligations.
- Compliance with common law or statutory obligations.
- To protect someone's life.
- For an organisation to complete its public task.
- So called 'legitimate interests', where personal data is used in ways individuals would reasonably expect it to be used and which have minimal privacy impact.
- Explicit consent based on a very clear and specific statement of consent by the individual. There are other rules around consent such as requiring positive opt-in and simplifying withdrawal of consent. Consent must only be used where the Group cannot rely upon an alternative lawful basis. Consent can be easily withdrawn with minimal notice.

3.3. All personal data shall be:

- Obtained and processed lawfully, fairly and transparently.
- Obtained for specified and legitimate purposes and shall not be further processed in any manner incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and kept up to date.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing as well as against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Not be transferred to another party, such as a company that processes our data on our behalf, or a business partner, unless they can provide evidence that they are compliant with the principles in section 3.1 and the principles by completion of the contract checklist, rights and requirements in section 2. All contracts with such parties shall include the standard terms that include compliance with data protection legislation or make reference to an established data sharing agreement.

3.4. Rights of individuals whose personal data is processed by the Group. Individuals have the right:

- To be informed about the collection and use of their personal data.
- To access their personal data and supplementary information.
- To have inaccurate personal data rectified or completed if it is incomplete.
- To have personal data erased.
- To request the restriction or suppression of their personal data.
- To obtain and reuse their personal data for their own purposes across different services.
- To object to processing based on 'legitimate interests'; for the purposes of direct marketing and for certain types of research.
- To challenge automated decision-making and profiling.

3.5. Personal data breaches

- Everyone involved with the Group has a responsibility to protect the

personal data of individuals that interact with the Group.

- All Group users are expected to be vigilant to the possibility of breaches of this policy. Users who become aware of, or even suspect such breaches must report the breach IMMEDIATELY to the Information Governance Manager.
- All Group users must be particularly vigilant to events that put personal data at risk of breaching any of the principles in section 2 and 3.1 of this policy. Such breaches are most likely to more commonly occur following a security breach of IT systems. But this is by no means the only way in which personal data may be at risk. There are strict timescales for reporting any such breach to affected individuals and the relevant authorities. It is therefore imperative that any actual or suspected breach is reported IMMEDIATELY to the Information Governance Manager.

## 4. Notification of data held and processed

4.1. All staff, students, clients and anyone about whom the Group processes personal data shall:

- Know what information the Group holds and processes about them and why.
- Know how to gain access to the stored data.
- Be aware of the procedures in place to keep the data up to date.
- Know what the Group is doing to comply with its obligations under Data Protection legislation and associated regulations.
- Know how to contact the Information Governance Manager and know how to lodge any complaint with the Information Commissioner's Office.

4.2. Human Resources shall ask every member of staff to review their personal data stored on the Human Resources database, annually using the HR self-service function.

4.3. Students wishing to check and update their records should do so by speaking to their pastoral tutor or visiting the student centre.

## 5. Responsibilities of staff

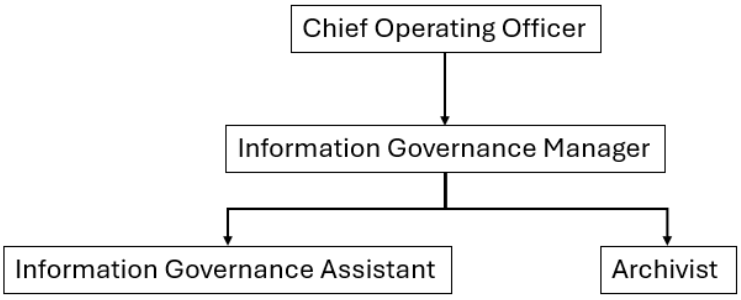
5.1. All staff shall be responsible for:

- Fully complying with the data protection principles, rights and requirements (3 & 4.1) in their handling of personal data.
- Performing a Data Protection Impact Assessment where new processing of personal data is planned.
- Promptly raising concerns about Data Protection or Data Security with the Information Governance Manager.
- Ensuring that all data that they provide to the Group in connection with their employment is accurate and up to date and that changes are either made direct onto HR self-service, where relevant, or are notified to Human Resources using the appropriate forms.
- Checking the information that the Group holds annually and correcting any errors.
- All staff are personally responsible for maintaining the security of personal data.

5.2. Any personal details of other people collected by a member of staff such as coursework marks or grades, references to employers or other academic institutions, or any matters about personal circumstances must be collected and stored in accordance with the guidelines included in the Staff Handbook, the Data Protection Policy and the Records Retention Policy.

## 6. Information Governance Framework

6.1. The Group's Information Governance is achieved through a structured approach as outlined by the following framework:




- The Information Governance Manager is the lead for Data Protection matters for the Group. For the purposes of Articles 37 - 39 of the UK GDPR, the Information Governance Manager is the designated Data Protection Officer of the Group.
- The Information Governance Team is comprised of the Information Governance Manager, the Information Governance Assistant and the Group's Archivist. The Information Governance team can be contacted via DP@chichester.ac.uk or by visiting the Information Governance office on the Chichester campus.
- Information Asset Owners are relevant members of staff who are responsible for one or more identified information asset(s). The Information Asset Owners are outlined in the Records Retention Policy.
- The Chief Operating Officer is the member of the Group Leadership Team responsible for executive oversight of information risks and information risk management.
- The Information Governance Manager makes monthly reports to both the Chief Operating Officer directly as well as the System Integration and Strategy Board with regards to information risks.

- The Chief Operating Officer then reports any notable information risks to the Audit & Risk Committee; the level of risk is set out in the Information Asset segment of the Group Ops Risk Register.

## 7. Data security

7.1. Staff are personally responsible for ensuring that any personal data they have acquired, manage, process, share, store or dispose of:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing accidentally or otherwise to any unauthorised third party.

7.2. All personal data must be kept in a locked filing cabinet or drawer. If it is stored on a computer, it must be stored securely with access only available to those who require it. Holding personal data on removable media or mobile devices is discouraged and the use of encryption is mandatory in these cases.

7.3. The official cloud storage solution for personal data is the Group Microsoft365 tenant and Docuware. A data protection impact assessment is mandatory prior to the use of any other cloud-based storage services.

7.4. The creation of new IT systems that include the storage of personal information shall have privacy included in the design process. The design shall include, but not limited to, the ability to log and manage the user access to the database and comply with data subject requests for access and erasure.

7.5. Students must ensure that all data supplied to the Group is accurate and up to date. Any changes in the data must be notified to Student Records or their Student Tutor.

## 8. International Data Transfers

8.1. The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations. These restrictions apply to all transfers, regardless of the size of transfer or how often data is transferred.

8.2. Restricted transfers must only be made where there is an adequacy agreement or the transfer is covered by appropriate safeguards or in exceptional circumstances, the transfer is covered under one of the UK GDPR article 49 exemptions. An exemption must not be used without prior consultation with the Information Governance Manager.

8.3. It should be noted following the Brexit transition period, the UK government determines which countries and territories are awarded adequacy status and these may differ from an adequacy status granted by the European Commission under EU GDPR.

## 9. Access to data

9.1. Persons on whom the Group holds data have the right to access any of the personal data that is processed about them. The request, known as a Subject Access Request (SAR), should be made to the Information Governance team and accompanied by a proof of identity (see Annex A). In most cases the SAR can be made free of charge. If a charge is appropriate then individuals will be contacted to arrange payment. The SAR must include enough information to enable the Group to find the personal data being requested, without excessive effort.

9.2. The Group will aim to comply with all requests for information as quickly as possible but will ensure that in all cases the details are provided within one calendar month unless the request is classed as complex in which case a request will be provided within three calendar months.

9.3. Any member of staff who receives or is otherwise made aware of a SAR, either verbally or in writing, must report it to the Information Governance team

immediately or at least within one working day of receiving it.

9.4. Personal information will never be disclosed over the telephone to outside bodies, or internal staff other than appropriate managers.

9.5. From time to time, it may be necessary to share personal data with other parties if there is a compelling need and a legal justification to do so which includes the protection of the vital interests of the person or if there is a public interest to do so. The method of transfer shall ensure the continued security of the data and be included within a pre-existing agreement (e.g. safeguarding teams).

## 10. Publication of information

10.1. It is the Group policy to make as much information public as possible. The following will be available to the public for inspection:

- Names and photographs of the members of the Corporation.
- Summary details of student achievement and examination successes.

  Details relating to an individual student will not be published without the express permission of that individual.
- Student participation in productions and events related to or resulting from their studies. Again, the permission of the individual would be obtained before this was done.

10.2. The Group internal phone list will not be a public document.

10.3. Any individual who has good reason for wishing that any of these details should remain confidential should contact the Information Governance team.

## 11. Subject consent

11.1. In accordance with Data Protection legislation, the Group will obtain consent from future students and new members of staff for the collection and processing of data unless there is an alternative lawful basis for processing the data. For the items described in the legislation as sensitive data, express consent will be obtained. This will include information about previous convictions and health needs. In cases where the applicants will be in contact with children and young people between the ages of 16 and 18 (and/or adults at risk), checks will be made, in accordance with the relevant statutes, to ensure that the people are suitable to work at the Group.

11.2. Enrolment and staff appointments will therefore become conditional on this consent being given.

11.3. The conditions for consent are set out in Article 7 of the GDPR. In the event a data subject's consent is used as the lawful processing for their personal data, staff should adhere to the following:

- adopt clear, straightforward language when requesting the data subject's consent.
- Data subject consent must be specific and informed, with data subjects being informed of:
    - the name of your organisation and the names of any other controllers who will rely on the consent – consent for categories of third-party controllers will not be specific enough;
    - why you want the data (the purposes of the processing);
    - what you will do with the data (the processing activities);
    - and that people can withdraw their consent at any time, as well as inform them how they can withdraw their consent.

11.4. Article 7(3) of the GDPR gives data subjects the right to withdraw their consent at any time; it must also be as easy to withdraw consent as it was to give it.

11.5. A record of the consent must also be logged by the Information Governance team and will be subject to a periodical refresh.

## 12. Processing sensitive information

12.1. For the purposes of operating the sick pay, equal opportunities, and other policies it is necessary to process sensitive information about a person's health, previous convictions, protected characteristics (age, ethnic origin, gender, religion or belief or disability), and other family details. The Group is aware that this could cause particular concern or distress and makes it clear why the information is being requested and how it will be used.

An article 9 condition, such as explicit consent is required prior to the collection and processing of sensitive personal data.

## 13. Data Processor

13.1. A 'Data Processor' is a person, public authority, agency or other body who carries out processing (which can be just viewing or holding) of personal data on the behalf of the Group. For example, a subcontractor providing training for our students.

13.2. There must be a contract in place stipulating equivalent levels of protection for personal data as those implemented by the Group and stipulated by data protection legislation. A template/contractual addendum for Data Processors is available from the Information Governance Manager.

13.3. The completion of a Data Impact Assessment is mandatory where there is a risk to the rights of individuals, before any data processor is engaged (see section 17). This includes the completion of the contracts checklist.

## 14. Data Controller

14.1. A Data Controller is an organisation that determines the purposes and means of the processing of personal data (decides why personal information will be collected and how it will be processed). The Group is ultimately legally responsible for the implementation of the data protection legislation.

## 15. Retention of data

15.1. The Group will keep some forms of data longer than others. However, information about staff, students and other stakeholders cannot be kept indefinitely.

15.2. The Group will maintain a separate retention policy listing key categories of data and how long they will be retained.

15.3. Any data reaching the end of its retention period will be securely and permanently disposed of. This will include both computer files and physical documents.

15.4. Any electronic media containing personal data must be securely disposed of at the end of its useful life (refer queries to IT Services).

15.5. Student records will be kept for a period in accordance with the retention policy. Student records include certain sensitive information that we are required to collect by Government funding bodies. This information includes ethnic origin and may include details relating to personal status. Further details may be obtained from the Information Governance team.

15.6. Staff records will be kept for a period in accordance with the retention policy. Information concerning pensions, taxation, potential or current litigation regarding the employment and details required for references will be kept for longer periods as determined by the specific circumstances. Documents related to health and safety issues will be kept for extended periods in certain circumstances such as for long term health concerns.

## 16. Cookies and similar technologies

16.1. Cookies are small pieces of data that are downloaded to a computer by a web site and allow the computer to be recognised by the web site on subsequent visits. They are often used for tracking of visitor activity or short-term uses such as maintaining shopping carts.

16.2. Legislation requires that consent is sought for the use of cookies for some purposes. The legislation covers not only cookies but any technology, which may leave data on a person's computer.

16.3. Any use of cookies or similar technology on externally facing Group web sites must be assessed against the legislation to decide whether consent from visitors is required.

## 17. Closed circuit television (CCTV)

17.1. The Group operates a CCTV system for the purposes of security and safety of both staff and students. The operation of this system complies with the Code of Practice issued by the Information Commissioner. Please refer to the CCTV policy.

17.2. Subject access requests for CCTV data will be dealt with in the same way as access to any other form of personal data (see section 7).

## 18. Release of personal data to official bodies

18.1. Occasionally official bodies such as the Police or Inland Revenue may request the disclosure of personal information. Except in emergencies, this will be referred to the Information Governance Manager or a person designated by the Information Governance Manager and assessed against the relevant sections of data protection legislation.

18.2. All requests for personal data by UK law enforcement agencies must be

accompanied by a signed 'request to external organisation for disclosure of personal data to the police form' otherwise known as a DP2. This form is provided by the law enforcement agency. Requests from international law enforcement agencies should be accompanied by the equivalent paperwork.

## 19. Data Protection Impact Assessments

19.1. A Data Protection Impact Assessment is essentially a risk management process and must be carried out prior to new uses of personal data in order to identify any issues related to Data Protection or related legislation.

19.2. Data Protection Impact Assessments must be formally documented and signed off by a relevant individual designated by the Data Controller prior to any new uses of personal data.

19.3. In this context "new uses of personal data" refers to use which is not already covered by the Group's existing ICO registration or existing formal consents acquired from data subjects.

19.4. A Data Protection Impact Assessment is a mandatory stage in the pre-planning of any new project involving use of personal data or any case where data is going to be processed by a data processor or joint controller on behalf of the Group.

19.5. In the event of a query about whether a Data Protection Impact Assessment is required you should consult the Information Governance team.

## 20. Artificial Intelligence

20.1. The use of any artificial intelligence (AI) that involves personal data must be subject to a full Data Protection Impact Assessment prior to deployment.

20.2. Whenever personal data is used by AI, due regard must also be given to Article 22 of the GDPR, which grants data subjects the right not to be subject to decisions based solely on automated processing, including profiling, if such decisions 'produces legal effects concerning him or her or similarly significantly affects him or her.'

## 21. Marketing use of personal data

21.1. In accordance with Data Protection legislation, the Group will obtain consent from individuals for the collection and processing of data for marketing purposes. For the items described in the legislation as sensitive data, express consent will be obtained.

21.2. Any requests for permission to market to an individual must be made on an "opt- in" basis.

21.3. All new proposals for processing personal data for marketing purposes shall be vetted by the Information Governance Manager.

## 22. Links to other policies

22.1. The Acceptable Use policy defines specific requirements in terms of data security.

22.2. The Records Retention Policy defines retention schedules and outlines requirements for the secure disposal of data assets.

## 23. Further information

23.1. For further information on the Data Protection Act 2018, UK GDPR and EU GDPR, please refer to the Information Commissioner's Office website.

## 24. Protection of Freedoms Act 2012

24.1. The Protections of Freedoms Act 2012 details the legal obligations relating to the storage, use and destruction of biometric data (for example, fingerprints and DNA). The Group does not store and use biometric data. More up-to-date mobile devices such as smart phones and tablets do make use of biometric data such as face and fingerprint recognition. This data is only stored on the device and should be wiped when the device is passed to another user.

## 25. Auditing

25.1. The Group will conduct documented audits, intended to test staff compliance with data protection policies and procedures as well as relevant data protection legislation. The audits will focus on particular areas or business processes and will include ad hoc compliance spot-checks.

25.2. Audits will be overseen by the Information Governance team and will be logged. Instances of non-compliance will be subject to follow-up checks after an appropriate interval.

25.3. Data processors and joint controllers will be audited using a risk-based approach proportionate to the type and volume of data they process on behalf of the Group.

## 26. Status of this policy

26.1. The operation of this policy will be kept under review by the Information Governance Manager.

26.2. This policy may be reviewed and varied from time to time by the Group Leadership Team.

**Annex A**

**Acceptable forms of identification**

In order to verify the identity of a person requesting personal information one form of identification from each category must be provided.

Photo identity

- Driving licence
- Passport
- Forces identity card

Proof of address

- Recent bank statement or utility bill etc.

| | |
|---|---|
| Policy review area | IT |
| Lead Manager/Owner | Mike Kemp |
| Approval level | Group Leadership Team/Corporation |
| Approval date | February 2025 |
| Review cycle | Every three years |
| Next review | September 2027 |