Data Protection Policy

1. Introduction

1.1. 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 in particular by reference to an identifier. Such identifiers are very wide and might include location data, or technology data, as well as the more obvious identifiers such as name.

1.2. 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 the policy can result in disciplinary proceedings.

1.3. 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 Data Protection Officer. If you have concerns, you can also refer to the Information Commissioner's Office Website.

1.4. 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.

1.5. 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.

1.6. 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. Prior to May 2018 the primary legislation was the Data

Protection Act 1998. After May 2018 new legislation came into force known as General Data Protection Regulation (GDPR).

1.7. It is a requirement that the Group is responsible for, and can demonstrate, compliance with the data protection principles detailed in section 3.1 below, and with the principles, rights and requirements for processing personal data in section 2 below.

2. Principles, Rights and Requirements for Processing Personal Data

2.1. The term "processing" in this context refers to all activities involving personal data such as (but not limited to) obtaining, storing, processing, sharing and disposing of personal data.

2.2. The Group must have a valid lawful basis for processing personal data in each and every case where this takes place. The available lawful bases are based on:

- Fulfilment of contractual obligations. The Group has invested in reputable legal advice in respect of contracts. This is in the form of a checklist, which should be completed for all new data processor contracts, and standard contractual terms, which may be requested from the Data Protection Officer.
- Compliance with common law of statutory obligation.
- Processing of personal data to protect someone's life.
- The exercise of public functions and powers that are set out in law.
- So called 'legitimate interests' where we use personal data in ways individuals would reasonably expect us to 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. The Group prefers not to rely on consent as the legal basis for processing personal data. Consent can be easily withdrawn with minimal notice.

2.3. 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 and 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 GDPR.

2.4. 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.

2.5. Personal data breaches

- Everyone involved with the Group now 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 Data Protection Officer.
- 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 Data Protection Officer.

3. Notification of data held and processed

3.1. 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.

3.2. 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.

3.3. Students wishing to check and update their records should do so by making a Subject Access Request (SAR), see section 6.1 of this document.

4. Responsibilities of staff

4.1. All staff shall be responsible for:

- Fully complying with the data protection principles, rights and requirements (2 & 3.1) in their handling of personal data.
- Performing a Privacy Impact Assessment where new processing of personal data is planned.
- Promptly raising concerns about Data Protection or Data Security with the Data Protection Officer.
- 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.

4.2. 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 and with the Data Protection Policy.

5. Data security

5.1. 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.

5.2. 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.

5.3. The official cloud storage solution for personal data is the Group OneDrive/Office365. A privacy impact assessment is mandatory prior to the use of any other cloud-based storage services.

5.4. 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.

5.5. 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 the Administration Office within the Directorate in which their studies are based.

6. Access to data

6.1. 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 Data Protection Officer 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.

6.2. 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 30 days.

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

6.4. 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 is in the public interest. The method of transfer shall ensure the continued security of the data and be included within a pre-existing agreement (e.g. safeguarding teams)

7. Publication of information

7.1. 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.

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

7.3. Any individual who has good reason for wishing that any of these details should remain confidential should contact the Data Protection Officer.

8. Subject consent

8.1. 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 legal 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.

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

9. Processing sensitive information

9.1. 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.

Explicit consent is required prior to the collection and processing of sensitive personal data.

10. Data Processor

10.1. A 'Data Processor' is someone 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.

10.2. 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 on ChiDrive.

10.3. A Privacy Impact Assessment is strongly advised where the rights of individuals may be at risk, and before any data processor is engaged. This includes the completion of the contracts checklist.

11. Datacontroller

11.1. A Data Controller is an organisation that 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.

12. Retention ofdata

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

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

12.3. 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.

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

12.5. 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 Data Protection Officer.

12.6. 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.

13. Cookies and similar technologies

13.1. 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.

13.2. Newly amended 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.

13.3. 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.

14. Closed circuit television (CCTV)

14.1. 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.

14.2. 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 6).

15. Release of personal data to official bodies

15.1. 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 Data Protection Officer or a person designated by the Data Protection Officer and assessed against the relevant sections of data protection legislation.

16. Privacy Impact Assessments

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

16.2. Privacy Impact Assessments must be formally documented and signed off by a person designated by the Data Controller prior to any new uses of personal data.

16.3. 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.

16.4. A Privacy 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 another company on behalf of the Group.

16.5. In the event of a query about whether a Privacy Impact Assessment is required then please contact the person designated for Data Protection queries by the Data Controller.

17. Marketing use of personal data

17.1. In accordance with Data Protection legislation, the Group will obtain consent from students and members of staff 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.

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

17.3. All new proposals for processing personal data for marketing purposes shall be vetted by the Data Protection Officer.

18. Links to other policies

18.1. The IT Security and the Acceptable Use of Computers and Telephones policies define specific requirements in terms of data security.

18.2. The Social Networking Policy provides guidance related to data protection whilst online.

19. Further information

19.1. For further information on the Data Protection Act 1998, refer to the guidelines on the Intranet or on the Information Commissioner's Office website.

20. Protection of Freedoms Act 2012

20.1. 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.

21. Auditing

21.1. Documented data protection audits will be carried out by a person nominated by the Data Controller. Audits will focus on particular areas or business processes and may include compliance spot-checks. The results of audits will be reported to the Data Controller.

22. There is also probably a scope for a section on International Transfer of data as we don't explicitly mention it. In essence we need a contract in place and some assurance that they adhere to our levels of DP in the handling of any data for which we are the data controller.

23. Status of this policy

23.1. The operation of this policy will be kept under review by the Chief Operating Officer.

23.2. It may be reviewed and varied from time to time by the Group Leadership Team.

23.3. This policy has been equality impact assessed.

Author:	Paul Drake, Group Data Protection Officer
Date approved:	May 2018
Approved by:	Group Leadership Team
Date reviewed:	April 2018
Date for review:	May 2020

Key Contact Information:

Paul Drake, Group Data Protection Officer. dp@chichester.ac.uk

Ben Phillips, Data protection Assistant. dp@chichester.ac.uk

Julie Sleeman, Chief Operating Officer.

Jon Dunster, Director of IT.

Annex B

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 license
- Passport
- Forces identity card

Proof of address

- Recent bank statement or utility bill etc.