DATA PROTECTION POLICY AND PROCEDURE

Policy category:	Technology and Data Protection
Approved by and when:	Policy Review Group Oct 2025
Policy owner:	Data Protection Officer
Related policies:	Policies listed in 6.1 of document
Applicable to:	Staff and students, visitors
Effective from:	October 2025
Review date:	30/09/2028

Document Version Control 1.0 – Revision History

Section	Summary of changes	Date updated
ALL	Update of College name, job titles, email addresses Update the list of privacy notices Added Data Access and Use Act	01/01/2025
3	Clarity on the definition of processing	01/01/2025
9.4	Changes to the lawful basis for processing – DUAA	01/08/2025
17.3	Confirmation that the College Group has a separate internal DSAR procedure document	01/01/2025
21	Additional explanation to the DPIA section to clarify when these documents are needed	01/01/2025
25.1	Update the transferring data outside the UK	
27.1	Added in the changes to the complaint process - DUAA	

Contents

1. Overview

1.1 University Centre Somerset College Group's reputation and future growth are dependent on the way the Colleges manages and protects personal data. Protecting the confidentiality and integrity of personal data is a key responsibility of everyone within the College Group.

1.2 As an organisation that collects, uses and stores personal data about its employees, suppliers, students, governors and visitors, the College Group recognises that having controls around the collection, use, retention and destruction of personal data is important in order to comply with the College's obligations under the Data Protection Laws and in particular its obligations under UK General Data Protection Regulation 2018, Data Protection Act 2018 and the Data (Access and Use) Act 2025.

1.3 The College Group has implemented this Data Protection Policy and Procedure to ensure all college staff are aware of what they must do to ensure the correct and lawful treatment of personal data. This will maintain confidence in the College Group and will ensure a successful working and learning environment for all.

1.4 The College Group needs to keep certain information about students for the purposes of discharging its contractual obligation to provide education and training, including monitoring performance and achievements and discipline. It is also necessary to process the information to comply with the College's statutory obligations (e.g. health & safety, child protection, safeguarding and disability discrimination legislation) and to discharge its obligations to its regulatory and funding bodies and government departments and agencies (e.g. the Education and Skills Funding Agency, OFSTED, Office for Students, Awarding Organisations, etc.).

1.5 The College Group may disclose personal data to the Education and Skills Funding Agency, OFSTED, Office for Students and such other statutory, regulatory and government bodies in accordance with the requirements referred to in the paragraph above.

1.6 The College Group may also disclose to a current or prospective employer or sponsor information relating to a data subject's attendance, performance, achievement and conduct.

1.7 The UK GDPR seeks to balance the protection of individual privacy with the business needs of the College. In order to achieve this balance, the College Group must comply with the principles relating to the processing of personal data which are set out in the regulations.

2. Policy Statement

2.1 This policy (and the other policies and documents referred to in it) set out the basis on which the College Group will collect and use personal data either where the College Group collects it from individuals itself or where it is provided by third parties. It also sets out rules and procedures on how the College Group handles, uses, transfers and stores personal data.

2.2 This policy does not form part of the formal contract for education or employment, but it is a condition of employment that employees will abide by the rules and policies made by the College Group. Any failure to follow the policy may therefore result in disciplinary proceedings.

3. Definitions

College Group – refers to University Centre Somerset College Group and includes all commercial businesses owned by the College Group.

College Group staff – any College Group employee, worker or contractor who accesses any of the College's personal data and will include employees, consultants, contractors and temporary personnel hired to work on behalf of the College Group.

Controller – any entity (e.g. company, organisation or person) that makes its own decision about how it is going to collect or use personal data.

A controller is responsible for compliance with Data Protection Laws. Examples of personal data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of personal data if it decides what personal data the College is going to collect and how it will use it.

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.

Data Protection Officer – Our Data Protection Officer can be contacted via email dpo@ucscollegegroup.ac.uk

EEA - Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK

IC – the Information Commissioner, the UK's data protection regulator. The College's entry on the Information Commissioner's Register of Data Controllers is Z4677243.

Individuals – living individuals who can be identified, directly or indirectly, from information that the College Group has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors, contractors and potential students. Individuals also include partnerships and sole traders.

Personal Data – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of personal data are given extra protection by Data Protection Laws.

Processor - any entity (e.g. company, organisation or person) which accesses or uses personal data on the instruction of a Controller. A Processor is a third party that

processes personal data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of personal data. Examples include: where software support for a system, which contains personal data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

Processing – is anything carried out with the data including holding and viewing data. It includes:

- obtaining
- holding
- amending
- collating and compiling
- reading and consulting
- disclosing
- transferring
- blocking, deleting or destroying information (data)

Special Categories of Personal Data – personal data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of personal data are subject to additional controls in comparison to ordinary personal data.

Criminal records data is information about an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.

4. Responsibility of Staff

4.1 All College Group staff must comply with this Data Protection Policy and Procedure.

4.2 College Group staff must ensure that they keep confidential all personal data that they collect, store, use and come into contact with during the performance of their duties.

4.3 College Group staff must not release or disclose any personal data outside the College;

or inside the College to recipients who are not authorised to access the personal data without the specific written authorisation from the Data Protection Officer.

4.4 It is compulsory for all staff to complete the College Group's online e-learning Data Protection briefing and undertake any additional training as appropriate.

4.5 It is the responsibility of staff as data subjects to inform the College Group of any changes to the information that they have provided in connection with their employment including changes of address or bank account details.

5. Student obligations

5.1 Students must ensure that all personal data provided to the College Group is accurate and up to date. They must ensure that any changes to their personal data is communicated to MIShelpdesk@ucscollegegroup.ac.uk

6. Relationship to Other Policies

6.1 This policy and procedure must be read in conjunction with the following policies:

- CCTV Policy
- Data Retention and Disposal Policy
- Freedom of Information Policy
- IT Acceptable Use Policy
- IT Security Policy
- Mobile Device Policy
- Mobile Phone Policy and Procedure
- Personal Data Breach
- Research and Ethics Policy
- Use of College's Emails
- Safeguarding and Child Protection Policy and Procedure
- Online Safety Policy

7. Accountability

7.1 As a publicly funded organisation, the College Group is required to appoint a Data Protection Officer (DPO). The DPO will report to Senior Management and the Governors of the College.

The duties of the DPO include:

- Informing and advised staff about their obligations to comply with the GDPR and other data protection laws by ensuring employees receive appropriate training and awareness communications
- Monitoring compliance with the GDPR and other data protection laws
- Managing internal data protection activities
- Advising on data protection impact assessments
- Conducting internal audits and investigations
- Investigating personal data breaches, recommending actions to reduce their impact and likelihood of recurrence
- Providing GDPR compliance updates to Senior Management and Board of Governors through the Audit Committee

7.2 The Head of Estates is responsible for ensuring that controls to manage the physical security of the College, including CCTV take account of relevant data protection laws and risks.

7.3 The Director of Funding and Operations is responsible for maintaining relevant student administration policies and procedures for the oversight of the management of student records and associated personal data across the College in compliance with data protection laws.

7.4 The Director of People and Culture is responsible for maintaining relevant human resources policies and procedures to support the compliance with data protection laws.

8. Data Protection Principles

8.1 In accordance with the requirements outlined in the GDPR and the Data Protection Act 2018, personal data must be:

1. **Processed lawfully, fairly and in a transparent manner** – The College Group must be transparent with individuals (data subjects) about how we will use their personal data. This is generally done through our Privacy Notices. The information that needs to be provided is set out in Article 13 and 14 of the GDPR.

2. **Collect for a specific purpose, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes** – Personal data must not be collected for one reason and then processed for another unless the College Group has informed the individual. The College Group's Privacy Notices will normally specify that some personal data may be used for a variety of purposes.

3. **Adequate, relevant and limited to what is necessary** – Personal data collected must be necessary for the purpose for which it is being processed and not to be collected 'just in case' and forms that are used to **collect** data will be reviewed to determine whether any sections can be made optional.

4. **Accurate and kept up to date** – This means that every reasonable step must be taken to ensure that personal data is inaccurate is erased or rectified as soon as possible.

5. **Kept for no longer than is necessary for the purpose for which it is being processed** – The College Group should not keep personal data for longer than it is needed. When personal data is no longer needed, it should be securely deleted/destroyed in accordance with the retention periods outlined in the Data Retention and Disposal Policy.

6. **Processed in a manner that ensures appropriate security of the personal data** – It is a requirement of the UK GDPR that appropriate technical and organisational security measures are used, monitored, controlled and audited to protect against unauthorised processing, accidental loss, destruction or damage to the personal data. The College Group takes the security of personal data very seriously and has in place policies, procedures and technologies to maintain the security of the data.

9. Lawful Use of Personal Data

9.1 The College Group lawfully processes personal data under the legal basis set out in Article 6 of the GDPR.

9.2 The majority of processing by the College is carried out because it is necessary for the performance of tasks carried out in the Public Interest. We limit the information we

collect to ensure we only collect what is needed to perform this duty. The College Group also seeks to obtain the consent from individuals for the purpose of College Group activities, where explicit consent is required.

9.3 The College Group will only share personal data with third parties as part of the statutory duties placed on us or as declared in the Privacy Notice. We do not share information about our learners with anyone without consent unless the law and our policies allow us to do so.

9.4 The recent Data Access and Use Act 2025 legislation has introduced a new lawful grounds for processing personal data. This development provides greater assurance for the College Group for processing personal data for important purposes including crime prevention, safeguarding, emergency response and other legitimate activities recognised under the Act.

10. Transparent Processing – Privacy Notice

10.1 Where the College collects personal data directly from individuals, the College will inform them about how the College uses their personal data. This is done via a privacy notice. The College has the following privacy notices:

- Staff
- Students and apprentices
- Recruitment and Selection
- Video Lesson Capture
- Employers

10.2 The Privacy Notices forms part of our new learner enrolment process and the new employee's induction process, and they are designed to ensure all learners and staff are fully informed of how their data will be used.

11. Data Quality – Ensuring the Use of Accurate, Up to Date and Relevant Personal Data

11.1 Data Protection Laws requires that the College Group only collects and processes personal data to the extent that it is required for the specific purpose(s) notified to the individual in a privacy notice (as above). The College Group is also required to ensure that the personal data the Colleges holds is accurate and kept up to date.

11.2 All College Group staff that collect and record personal data shall ensure that the personal data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of personal data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

11.3 All College Group staff that obtain personal data from sources outside the College Group shall take reasonable steps to ensure that the personal data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

11.4 In order to maintain the quality of personal data, all College Group staff that access personal data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to personal data which the College Group must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

11.5 The College Group recognises the importance of ensuring that personal data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The College Group has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the College responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their personal data should be dealt with in accordance with those documents.

12. Personal Data must not be kept for longer than needed

12.1 Data Protection Laws require that the Colleges do not keep personal data for longer than is necessary for the purpose or purposes for which the College collected it.

12.2 The College has assessed the types of personal data that it holds and the purposes it uses it for and has set retention periods for the different types of personal data processed by the College as set out in the Data Retention and Disposal Policy.

13. Credit Card Information Handling

13.1 The College Group will destroy all cardholder information in a secure method when no longer required. Media containing card information must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable.

13.2 It is prohibited to record the contents of the credit card magnetic stripe (track data) on any media whatsoever.

13.3 It is also prohibited to record the card-validation code (the 3 or 4 digits printed on the back of the card) on any media whatsoever including paper records.

13.4 All but the last four number of the credit or debit card account number must be masked (i.e. X's or *s) when the number is displayed electronically or on paper.

14. Data Security

14.1 Security of personal data is extremely important to the College Group. We are trusted to protect sensitive information that may be supplied while conducting business.

14.2 Special category data is regarded by the UK GDPR as more sensitive and requires additional protection and can only be processed where there is a lawful basis to do so.

14.3 Under Article 6 of the UK GDPR the College Group processes personal data relating to an individual's ethnic origin. Processing is carried out in the exercise of the College Group's official authority and in compliance with statutory obligations to which the College Group is subject.

14.4 The College Group will maintain the Cyber Essentials Accreditation as a minimum standard to demonstrate our IT Security Management Systems are effective.

14.5 **Clear Desk Arrangements -** The College Group encourages a 'clear desk' approach for those involved in handling personal data in the course of their duties. All staff with access to personal data should ensure that when work areas ae unattended, no personal data or sensitive information is left unsecured.

14.6 Electronic personal data should be:

- stored on the College Group's central servers
- password protected
- securely encrypted if transferred to any other form of storage device e.g. laptop
- deleted at the end of its retention period or when no longer required.

14.7 Through regular training and awareness raising, the College Group will seek to minimise the amount of unstructured data in use and only where there are valid reasons to do so will this data be shared.

14.8 Under no circumstances should personal data be stored at staff members' homes whether in manual or electronic form, on laptop computers or other personal portable device.

15. Working from home and use of video conferencing/lessons

15.1 Staff working from home using the College Group Microsoft Office 365 account must ensure the same level of data security is applied and not downloaded to personal devices.

15.2 The College Group will use video conferencing facilities in order to hold meetings for staff and lessons for students virtually where possible. When these are recorded, the organiser of the meeting will inform those involved in the meeting/lesson that it is being recorded and the reason(s) why. Consent can be refused or withdrawn at any time.

15.3 If under exceptional circumstances, personal data is taken home for staff to process that data, the personal data will be confirmed by the Head of Department and logged so that no data is lost.

15.4 Staff are instructed to use College Group's provided equipment where possible. Where this is not possible and staff use their own devices, that personal data is stored on OneDrive and not on the individual's personal device.

16. Data Breaches

16.1 The College Group has a Data Breach Policy and Procedure in place to both mitigate

the risk of a breach occurring and to ensure that there are appropriate procedures in place to respond.

16.2 The College Group expects its employees to embed security and prevention practices in their normal working day to ensure personal, or special category data is protected for the purposes of college business.

16.3 Staff are responsible for taking all necessary steps to ensure that no breaches of information result from their actions. If a member of staff suspects that a breach of data has occurred or a near miss, it is their responsibility to report immediately to the Data Protection Officer (DPO) dpo@ucscollegegroup.ac.uk so that appropriate action can be taken to minimise harm results from the breach.

16.4 All breaches large or small, regardless of the harm or potential harm, should be identified and reported to the DPO. Failure to follow correct procedure or ignoring a possible breach may result in a disciplinary action.

17. Individuals' Rights

17.1 UK GDPR gives individuals more control about how their data is collect and stored and what is done with it. Some existing rights of individuals have been expanded upon, and some new rights have been introduced.

17.2 **Right to be Informed/Sharing Personal Data (Privacy Notice)**

The UK GDPR requires the College Group to inform individuals of our personal data processing activities, and we do this through Privacy Notices as explained in Point 10 above.

17.3 **Right of Access**

Individuals have the right to obtain confirmation that their data is being processed and the right to submit a **Data Subject Access Request (DSAR)** to gain access to their personal data in order to verify the lawfulness of the processing or obtain copies of the records for other purposes. DSAR should be made via the Data Protection Officer email dpo@ucscollegegroup.ac.uk The DPO and staff will follow the College Group's DSAR procedure document.

Further information on how to make a DSAR request, together with information on

Third Party Requests and Police/Enforcing Agencies are available on the Group website.

The DPO will maintain a DSAR register which is reported termly to Senior Management and Governors.

17.4 **The Right of Rectification and Restriction**

Individuals have the right to request the College Group to block, or suppress processing of, their personal data. Individuals are also entitled to have personal data held by the College rectified if it is inaccurate or incomplete.

Where a restriction may affect the College Group carrying out their legal or contractual obligations or it is believed that the data is being processed under the Public Interest, Vital Interest or Legitimate Interest conditions, the College will follow guidance from the IC to determine whether the request is valid.

If a request is determined to be valid, the College Group will take steps to immediately restrict processing of personal data.

Requests for rectification of data should be made to MIS helpdesk by email MIShelpdesk@ucscollegegroup.ac.uk

17.5 **Right of Erasure (Right to be Forgotten)**

Individuals have the right to request the erasure (deletion) or removal of personal data where there is no lawful basis for its continued processing in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there are no overriding legitimate interests for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with legal obligation

- In a marketing context, there personal data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time.

Where the individual objects, the personal data must not be processed for such purposes.

The College Group has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, historical research or statistical purposes
- The exercise or defence of legal claims
- Where personal data has been used for printed materials such as marketing leaflets and prospectuses, the College Group may no longer have control once published and therefore may not be able to exercise the right to erasure. Where this is likely to apply, the College will state this in our request for consent.

17.6 **Right to Data Portability**

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract

The College Group is not required to adopt or maintain processing systems, which are technically compatible with other organisations. If the personal data concerns more than one individual, the College will consider whether providing the information would prejudice the rights of any other individual.

Personal data will be provided in a structured, commonly used and machine-readable form, and where feasible, data will be transmitted directly to the other organisation at the request of the individual.

17.7 **Right to object**

The College Group may stop processing an individual's personal data if they object to processing based on legitimate interests or a task in the public interest / exercise of official authority (including profiling).

The College Group will stop processing personal data for direct marketing or for research/statistical reasons if a data subject requests so.

17.8 **Rights in relation to automated decision making and profiling**

The College Group will not undertake automated decision making or process personal data for the purpose of profiling individuals.

18. Closed Circuit Television (CCTV)

The College Group uses CCTV in various locations to ensure it remains safe. The College Group will adhere to the IC's code of practice for the use of CCTV. The College does not need to ask individuals' permission to use CCTV, but the College Group makes it clear where individuals are being recorded. Security cameras are clearly visible and are accompanied by prominent signs explaining that CCTV is in use.

19. Marketing and Consent

19.1 Marketing consists of any advertising or marketing communication that is directed to particular individuals. The College Group uses a variety of marketing techniques to attract learners, employers and the public to the services and activities the College Group offers.

19.2 The College Group can contact individuals to send them marketing or promote the College Group, but when this is carried out, it will only be done in a legally GDPR compliant manner where the College Group has obtained consent.

19.3 We will keep records documenting how and when consent was given, these may be held in a variety of storage mechanisms depending on the type of data and/or consent required. This information will be readily available for staff to check that consent has been obtained e.g. use of student profile photographs.

19.4 The College Group provides more details in the student privacy statement, learning agreements and consent forms when profiling or photography take place where an individual's consent is a 'clear affirmative action' to be contacted for marketing purposes.

19.5 The College Group is aware of the Privacy and Electronic Communications Regulations (PECR) alongside data protection. The PECR applies to direct marketing and to any electronic communication the College Group sends out including telephone calls, emails and text messages.

20. Photography and Videos

20.1 As part of the activities that take place on campuses, the College Group may take photographs and record images of individuals. The College Group will obtain verbal consent of general photographs used for social media. Written consent will be obtained for any face-to-face profile photography or videos of staff or students for marketing and promotional materials.

20.2 Uses may be (but not limited to):

- Internal or external promotional material such as notice boards, magazines, brochures, social media
- External of the College Group by external agencies
- Online on College Group websites or social media pages

20.3 Consent can be refused or withdrawn at any time. If consent is withdrawn, the College Group will delete the photograph or video and not distribute it further. When using photographs and videos in this way the College Group will not accompany them with any other personal information about the learner, to ensure they cannot be identified unless this has been explicitly agreed beforehand, for example on posters describing a learner's journey and progression route.

21. Data Protection Impact Assessments (DPIA)

21.1 A DPIA will be carried out for a new service, system, product or process involving personal data. This must be completed prior to the processing of the data.

21.2 Risks created by the College Group's data processing activities are continuously monitored through the Group's risk register in order to identify when a type of processing is likely to result in a high risk to the rights and freedoms of individuals.

21.3 Where the likelihood that the rights and freedoms of individuals may be infringed is assessed as 'high' or above the DPO will arrange for a DPIA to be undertaken.

The DPIA will incorporate the following steps:

- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the assessment outcomes
- Integrate the outcomes

22. Data Sharing

22.1 When personal data is shared internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected. If the personal data is shared internally for a new and different purpose(s), the student will be informed.

22.2 The College Group aims to comply with the code of practice on data sharing issued by the IC. When personal data is transferred externally, and legal basis must be determined and an information sharing agreement between the College and the third party must be completed.

22.3 The College Group does not require the consent of a student to share their personal data for the purpose of complying with:

- Its contractual obligations to the Education and Skills Funding Agency and successor organisations
- Its legal obligations under the education acts and safeguarding legislation

22.4 The College Group may share personal data without the individual's knowledge, where,

for example, personal data is processed for the:

- prevention or detection of crime
- apprehension or prosecution of offenders or
- assessment or collection of tax or duty.

22.5 **Disclosure of personal data to employers** – many students attend College Group under the sponsorship of their employer. This may include paid time to attend or payment of fees. These students will be required to consent to the sending of routine reports to their employers on academic progress and attendance as part of their consent on the application and enrolment form.

23. Examination Marks

23.1 Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide.

24. Research Data

24.1 Before commencing any research which will involve obtaining or using personal data and special categories of personal data, the researcher must give proper consideration to this policy and the Research and Ethics Policy. The researcher must ensure that the fairness, transparency and lawfulness principle is complied with and that privacy by design and default is applied. This means that wherever feasible, research data must be anonymised or pseudonymised at the earliest possible time.

25. Transferring Personal Data to a Country Outside the UK and EEA

25.1 Data protection law places strict controls on transferring personal data outside the UK. This includes any storage or access to personal data from outside the UK or EEA. The College Group must consider this when appointing any supplier based overseas, or where a supplier's group companies may allow staff outside the UK to access the data.

25.2 College Group staff must not export any personal data outside the UK without the approval of the Data Protection Officer.

25.3 The College Group does not transfer any personal data outside the UK. If this changes, the transfer (including access to it) will be based on one of the following safeguards: an EU Adequacy decision (recognised by the UK), EU Standard Contractual Clauses (SCCs) and the UK Addendum to EU SCCs. Please check this policy and the Privacy Policy for any relevant updates.

26. Requests for Information under the Freedom of Information Act

26.1 The Freedom of Information Act 2000 imposes a number of obligations on public authorities, which for these purposes includes the College, and provides the public with wide rights of access to the College's records. Any person who wishes to exercise this right should apply in writing to the Freedom of Information Act Officer.

26.2 For most requests the College Group will issue no charges. However, where the quantity of work required to satisfy the request exceeds reasonable limits the College Group will either refuse or provide the information or charge for its collation.

27. Complaints

27.1 Under the Data Access and Use Act, the College Group is required to handle complaints from individuals who are concerned about the way their data is used breaches the data protection legislation. Any person to who believes that the College Group has not complied with legislation should notify the Data Protection Officer dpo@ucscollegegroup.ac.uk who will follow the College Group's complaints procedure.

27.2 If the complainant is still unhappy with the College's response or needs any advice, they should contact the IC on the IC helpline 0303 123 1113 or go to the IC website

28. Review of Policy

28.1 The Data Protection Policy and Procedure will be reviewed in line with future legislative changes, case law or at no later than two years after the issue date.

28.2 The planned review date for the Data Protection Policy and Procedure is October 2028. However, the Policy and Procedure will be updated before this if there are changes to the legislation.