



UCG Managing Data Subject Right Requests Policy

This policy outlines how the United Colleges Group will process data subject requests (for City of Westminster College and the College of North West London).

Document Status	
Owner	Amanda Thorneycroft
Author	Gora Selliah
Date of Origin	22/03/2024
Colleges covered	City of Westminster College, College of North West London
Version	0.4
Date of Approval	09 December2024
Date of Next Review	December 2027
Approval Body	UCG Corporation

CONTENTS

1.	3	
2.	4	
3.	5	
4.	5	
5.	5	
	MANAGING DATA SUBJECT REQUESTS	6
6.	6	
7.	6	
8.	6	
9.	7	
10.	7	
11.	8	
12.	9	
13.	9	
14.	9	
15.	10	
16.	10	
17.	10	
18.	11	
19.	11	
	19.1	11
	19.2	12
	19.3	12
	19.4	14
	19.5	14
20.	16	
21.	16	
22.	17	
23.	18	
24.	19	
25.	20	
26.	21	

27. 21
28. 22









1. REFERENCED TERMS AND DOCUMENTS

Document	Details
Employees	Includes <i>Staff, Contractors and Consultants</i> .
Authorised employee	Alludes to <i>the Privacy and any other employee authorised as such by the Privacy team</i> . For the UCG Authorised Employees List see <i>Appendix 2</i> .
General Data Protection Regulation (GDPR)	Means the EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC).
DPA	Means the UK Data Protection Act 2018
Data Subject	Means an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Subject Request	Means a request from an individual data subject or from someone acting with the authority for the individual, e.g., a parent making a request in relation to information relating to their child or a lawyer appointed to act on their behalf.
Personal Data	Means any information relating to an identified or identifiable natural person ('data subject').
United Colleges Group Data Protection Policy	Data and Privacy (ucg.ac.uk)

<p>United Colleges Group Data Protection / Privacy team</p>	<p>Privacy team is comprised of:</p> <p>Data Privacy Team: gdpr@ucg.ac.uk GRCI Law (DPO): dpoas@grcilaw.com Gora Selliah: gora.selliah@cw.ac.uk Iqbal Khan: iqbal.khan@cw.ac.uk</p>
---	---

2. INTRODUCTION

2.1 The General Data Protection Regulation (GDPR) grants data subjects certain rights regarding their personal data including the right to:

	<p>Information</p>
	<p>Access their personal data.</p>
	<p>Correct their personal data.</p>
	<p>Erase their personal data.</p>
	<p>Restrict personal data processing about them.</p>
	<p>Receive a copy of certain personal data or transfer that personal data to another data controller, also known as the data portability, right.</p>
	<p>Object to personal data processing.</p>
	<p>Not be subject to automated decision-making in certain circumstances.</p>

2.2 This document sets out the key features regarding handling or responding to data subject right requests made by data subjects or their representatives.

3. SCOPE

- 3.1 This document applies to all employees but much of it is aimed primarily at those employees who are authorised to handle data subject right requests. These sections are identified by the words 'authorised employees' appearing in the section title. For other employees, it provides guidance on what to do if you receive a data subject right request.
- 3.2 This policy and procedure include all data subjects about whom United Colleges Group holds personal data and all personal data held on all college information systems, whether hosted on site or in the cloud, on portable storage media or devices or paper.
- 3.3 The purpose of this document is to outline the steps United Colleges Group as Data Controller takes when it receives a request from a data subject to exercise their rights in accordance with the General Data Protection Regulation (GDPR).

4. RESPONSIBILITY

- 4.1 All employees are responsible for ensuring that they recognise a data subject right request and to forward it or direct the requestor onto the Data Privacy Team (gdpr@ucg.ac.uk) immediately.
- 4.2 Any questions regarding this document should be addressed to the Data Privacy Team.
- 4.3 If United Colleges Group acts as a data controller towards the individual making the request, then the data subject right request will be addressed based on the provisions of this procedure.
- 4.5 If United Colleges Group acts as a data processor the Data Privacy Team will forward the request to the appropriate data controller on whose behalf United Colleges Group processes personal data of the relevant data subject.
- 4.6 The overall responsibility for ensuring compliance with a data subject right request rests with the Chief Financial Officer.

5. PURPOSE

- 5.1 The purpose of this policy is to set out how to do the following:
- Confirm the identity of the data subject making a request and (where applicable) the identity of a third party who may be making a request on a data subject's behalf.
 - Record and track data subject requests and responses, including all correspondence and internal documents related to requests.
 - Determine whether a condition or exemption exists that permits or requires us to refuse to fulfil the request.
 - Handle data subject requests that involve several data subjects' personal data.
 - Communicate with data subjects at reasonable intervals regarding the status of their request.

MANAGING DATA SUBJECT REQUESTS

6. DATA SUBJECT REQUEST SUBMISSION FORMAT

- 6.1 The employee should always encourage the requestor to submit the request in writing using the *UCG Data Subject Access Request Form* (see Appendix 1) to provide a clear audit trail of the data subject request and to ensure that both the requestor and United Colleges Group have a clear record of what was requested. The form asks data subjects for specific information necessary to process and respond to their request. Note that the requestor can submit a request in whatever format they choose.
- 6.2 In the event of a verbal data subject request for example by telephone, the employee should direct the individual to submit the request in writing using the *UCG Data Subject Access Request Form* (see Appendix 1) via email or postal mail to the address: *The Data Privacy Team, United Colleges Group, 25 Paddington Green, London W2 1NB.*
- 6.3 If the individual advises that a written request is not possible, the Data Privacy Team will liaise with them to facilitate an alternative method of submission.
- 6.4 **All data subject rights requests should be immediately directed to the Data Privacy Team (gdpr@ucg.ac.uk).**

7. HOW TO RECOGNISE A DATA SUBJECT REQUEST (ALL EMPLOYEES)

- 7.1 A request will typically be made in writing but may be made verbally e.g., via telephone or in person. The request may refer to the GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so to be a valid request. A letter which *states 'please provide me with a copy of all the information that you have about me' or 'delete everything you have on me'* will be a data subject request and should be treated as such.
- 7.2 If you are in any way unsure as to whether a request is a data subject rights request, please contact the Data Privacy Team.

8. WHAT TO DO WHEN YOU RECEIVE A DATA SUBJECT REQUEST (ALL EMPLOYEES)

- 8.1 If you receive a data subject request and you are not authorised to handle it, you must immediately take the steps set out below. There are limited timescales (1 calendar month) within which United Colleges Group must respond to a data subject request and any delay could result in United Colleges Group failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected data subject.
- 8.2 The timescales referred to in this procedure must be calculated from the day you receive a Data Subject Request (whether it is a working day or not) until the corresponding calendar date in the next month, for example if a request is received on 12 April, information must be provided by 11th May.
- 8.3 Upon receipt of a Data Subject Request, you must immediately forward the request to the Data Privacy Team.

Format	Action
Email	If the Data Subject request was received by email, you must immediately forward the request to the Data Privacy Team at gdpr@ucg.ac.uk
Letter	If you receive a Data Subject Request by letter you must: <ol style="list-style-type: none"> 1) Scan the letter. 2) Send the original to the Data Privacy Team at the following: Gora Selliah, City of Westminster College, 25 Paddington Green, London W2 1NB 3) Send a scanned copy of the letter to the DPO (dpoaas@grcilaw.com) and Ryan Peeney (rpeeney@grcilaw.com)
Verbally	If you receive a verbal Data Subject Request, you must: <ol style="list-style-type: none"> 1) Take the name and contact details of the individual. 2) Inform the individual verbally that you will notify the Data Privacy Team that the individual has made a verbal request and that the Data Privacy Team will contact them in relation to the request. 3) Immediately email the Data Privacy Team at gdpr@ucg.ac.uk providing the individual's contact details and details of the verbal request and the date on which it was received.

8.4 You will receive confirmation when the request has been received by the Data Privacy Team. If you do not receive such confirmation within two working days of sending it, you should contact the Data Privacy Team to confirm a safe receipt.

8.5 You must not take any other action in relation to the data subject request unless it is set out in this document, or the Data Privacy Team has authorised you to do so in advance and in writing.

9. **ACKNOWLEDGING RECEIPT OF DATA SUBJECT REQUESTS (AUTHORISED EMPLOYEES)**

The Data Privacy Team will acknowledge the Data Subject Request and where the Data Subject (or their representative) has not done so, suggest that the requestor complete a Data Subject Request form to better enable United Colleges Group to locate the relevant information. The requestor does not need to complete the form for the Data Subject Request to be processed. For the *UCG Authorised Employees List* see Appendix 2.

10. **TRACKING DATA SUBJECT REQUESTS**

10.1 All Data Subject Requests will be logged via the Rights of Data Subjects Register.

10.2 The Data Privacy Team must continuously track the following regarding data subject requests via the Rights of Data Subject Register located in the Data Privacy Team's college SharePoint site.

- Receipt date of data subject request.
- Data subject name.
- Requester name (if applicable).
- Assigned employee(s) that will handle data subject request.
- Request status (new, in progress, completed).
- Request format.
- Method(s) of identification.

- Data subject ID.
- Request type.
- Request details.
- Interim response date(s) (if applicable).
- Final response date.
- Final response.

10.3 The Data Privacy Team must maintain all correspondence and documentation related to data subject requests in the United Colleges Group DSAR Register and Data folder on the college's SharePoint site. Access to DSAR correspondence and documentation is limited to the Data Privacy Team.

11. PROOF OF DATA SUBJECT'S IDENTITY (AUTHORISED EMPLOYEES)

11.1 The authorised employee must check the identity of anyone making a Data Subject Request to ensure information is only given to the person who is entitled to it. The request for ID must be fair and proportionate. If the DSAR request is from a current employee, you may not wish to ask for ID. For the *UCG Authorised Employees List* see Appendix 2.

11.2 If a Data Subject makes a request electronically with a username or other unique identifier and a password, additional documents to prove the data subject's identity is unlikely to be not necessary however seek advice from the Data Privacy Team before proceeding.

11.3 The authorised employee shall check the identity of anyone making a Data Subject Request that cannot verify their identity online through a username or unique identifier and password and must ensure information is only given to the person who is entitled to it. If the identity of a Data Subject Request requestor has not already been provided, the authorised employee will ask the requestor to provide two forms of identification, one of which must be a photo identity. The other can be confirmation of address or date of birth. The request for ID must be fair and proportionate so for example, a UK Driver's License showing date of birth, address and a photo would be fine. Student ID cards would be acceptable as well.

11.4 If the authorised employee cannot verify the Data Subject's identity based on the information provided, or if the Data Subject did not include all the required forms of identification, the authorised employee must advise the Data Subject in writing via postal mail, or electronically via email that United Colleges Group needs additional information to verify the data subject's identity.

11.5 The authorised employee must store all identification documentation in the United Colleges Group DSAR Register and Data folder and only use the identification documentation provided to identify the Data Subject to be able to respond to the Data Subject Request and not for any other purpose. The authorised employee must delete or destroy all identification after the Data Privacy Team has confirmed that they are satisfied with the verification of the Data Subject's identity.

11.6 The authorised employee should make clear when communicating with the Data Subjects that the time frames to respond to a Data Subject Request does not start until United Colleges Group has received proof of identity.

11.7 If, having requested additional information, United Colleges Group is still not able to identify

the Data Subject, United Colleges Group may refuse to act on a Data Subject Request.

12. REQUESTS MADE ON DATA SUBJECT’S BEHALF (AUTHORISED EMPLOYEES)

- 12.1 A third party may make a request on a Data Subject’s behalf. The authorised employee should request proof of the Data Subject and the third party’s identity and evidence of the third party’s legal right to act on the Data Subject’s behalf, e.g., written authority from the Data Subject. For the *UCG Authorised Employees List* see Appendix 2.
- 12.2 The authorised employee must verify the requestor’s identity and, where applicable, any proof of legal authority to act on the Data Subject’s behalf based on the information provided. If the authorised employee cannot verify a third party’s legal authority to act on the Data Subject’s behalf, they must advise the third party in writing of the additional information needed to confirm the legal authority.
- 12.3 Third party requestors who cannot provide this will be refused until such time that they can.

13. THIRD PARTY INFORMATION REQUESTS NOT MADE ON THE DATA SUBJECT’S BEHALF (AUTHORISED EMPLOYEES)

- 13.1 Requests for information about a Data Subject made by third parties who are not acting on behalf of the Data Subject will be accepted, but they must be accompanied a letter showing their written authority to make such requests, e.g., Police and Law Enforcement agencies must state the exemption to the right to access under the UK Data Protection Act 2018 that they believe entitles them to access information. For the *UCG Authorised Employees List* see Appendix 2.
- 13.2 The Data Privacy Team shall consider the validity of any request of this nature.

14. IDENTIFYING AND LOCATING RELEVANT PERSONAL DATA

- 14.1 The Data Privacy Team is responsible for leading the effort to locate personal data relevant to a Data Subject Request and must:
 - 14.1.1 Identify all departments that might reasonably be considered to hold personal data relevant to the request.
 - 14.1.2 Work with the IT department to collect the personal data about the Data Subject from all relevant sources including:
 - Emails, electronic files and documents, and electronic systems.
 - Databases.
 - Automated systems such as door entry or key card access systems.
 - Word processing systems.
 - Computer hard drives.
 - Hard copy files.
 - Voice recordings.
 - Photographs.
 - Monitoring records and CCTV images.
 - Internet logs.
 - Telephone records.
 - Back-up files.
 - Third-party data processors’ systems.
 - Other relevant sources.

- 14.2 The Data Privacy Team must review the files and the documents collected and identify whether the information gathered is personal data relevant to the request.
- 14.3 If the scope of the Data Subject Request is unclear or does not provide sufficient information to conduct a search, then the Data Privacy Team must communicate to the Data Subject that they need more specific information to process the request and locate the relevant personal data and indicate the information needed. Clarification must be done as soon as possible. It is possible to use “Stop the Clock” which will pause the timeline until a response is received.
- 14.4 The Data Privacy Team must retain internal documents that show the steps and efforts made to locate relevant personal data, including all the search methods used.

15. TIME TO RESPOND TO DATA SUBJECT REQUESTS

- 15.1 The Data Privacy Team must respond to a Data Subject Request within the timescale set out in paragraph 8.2 above.
- 15.2 If the Data Privacy Team determines that a Data Subject Request may take longer than 30 days to respond to, the Data Privacy Team may escalate to the Data Protection Officer (“DPO”). The DPO must determine if United Colleges Group can extend the 30-day response time.
- 15.3 If United Colleges Group extends the period for responding to the Data Subject Request the Data Privacy Team must inform the requester within 30 days of receipt of the Data Subject Request of the extension and explain the reason for the delay.

16. DATA SUBJECT RESPONSE (AUTHORISED EMPLOYEES)

- 16.1 Information should be provided to the Data Subject in response to their Data Subject Request:
 - 16.1.1 Using United Colleges Group’s standard form response, wherever possible.
 - 16.1.2 In a way that is concise, transparent, easy to understand and easy to access.
 - 16.1.3 Using clear and plain language, with any technical terms, abbreviations or codes explained.
 - 16.1.4 In a commonly used electronic format, if the Data Subject Request was made electronically, unless otherwise requested by the requestor.
 - 16.1.5 Where possible, by providing remote access to a secure system which would provide the requestor with direct access to the personal data, where there is a large volume of data.

17. GENERAL REASONS FOR DENYING A DATA SUBJECT REQUEST

- 17.1 The Data Privacy Team must determine if United Colleges Group has a basis not to respond to a Data Subject Request. United Colleges Group may refuse to respond to Data Subject Requests for the following reasons:
 - 16.1.1 A third party fails to present sufficient proof of authority to make the request on the Data Subject’s behalf.
 - 16.1.2 Where United Colleges Group processes data for purposes that do not require data subject identification and United Colleges Group demonstrates that it cannot identify the Data Subject, unless the Data Subject provides additional information enabling identification.
 - 16.1.3 National law provides a basis for denying the request.
 - 16.1.4 United Colleges Group demonstrates that the request is manifestly unfounded or

excessive, in particular because of its repetitive character.

- 16.1.5 United Colleges Group does not hold any personal data related to the Data Subject Request.
- 17.2 These general grounds are in addition to the specific grounds for denying a request made under GDPR (as included in the UK DPA 2018) Articles 15 (right to access), 16 (right to rectification), 17 (right to erasure), 18 (right to restrict processing), 21 (right to object to processing), and 22 (automated processing exception) of the GDPR.
- 17.3 Where United Colleges Group refuses to respond to a Data Subject Request, the Data Privacy Team must explain the refusal to Data Subjects without undue delay and at the latest within 30 days after receipt of the request (unless a determination is made to extend the response deadline) and advise them of their right to complain to the supervisory authority and seek a judicial remedy.
- 17.4 If United Colleges Group does not have or process personal data related to the Data Subject, the Data Privacy Team should indicate that United Colleges Group conducted a diligent search for records related to the Data Subject's request and did not uncover responsive results. The Data Privacy Team should retain internal documents for 6 months after the last communication with the requestor that show the steps United Colleges Group took to locate relevant personal data, including all the search methods used.

18. FEES FOR RESPONDING TO DATA SUBJECT REQUESTS

- 18.1 Usually there is no charge for United Colleges Group to comply with a Data Subject Request.
- 18.2 United Colleges Group may charge a fee based on the reasonable administrative costs of complying with the Data Subject Request if:
- It is manifestly unfounded or excessive.
 - A Data Subject requests additional copies of their data.
- 18.3 The fee will be calculated based on the administrative cost of providing the information.
- 18.4 The Data Privacy Team shall contact the requestor promptly and inform them that United Colleges Group has decided to charge a fee and does not need to comply with the Data Subject Request until the fee has been received.

SPECIFIC DATA SUBJECT RIGHT REQUESTS

19. PERSONAL DATA SUBJECT ACCESS REQUESTS (DSARs)

19.1 General

- 19.1.1 A personal Data Subject Access Request (DSAR) is a request from an individual Data Subject (or from someone acting with the authority for the individual, e.g. a parent making a request in relation to information relating to their child or a lawyer appointed to act on their behalf):
- For confirmation as to whether United Colleges Group processes personal data about the Data Subject and, if so
 - For access to that personal data, and
 - Certain other supplementary information

19.1.2 A Data Subject is entitled to receive access to the personal data United Colleges Group processes about the individual and the following information:

- The purposes for which United Colleges Group processes the data.
- The recipients or categories of recipient to whom the personal data has been or will be disclosed, where those recipients are in third countries or international organisations.
- Where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The fact that the individual has the right:
 - (i) To request that United Colleges Group rectifies, erases, or restricts the processing of the individual's personal data.
 - (ii) To object to its processing.
 - (iii) To lodge a complaint with the ICO.
- Where the personal data has not been collected from the individual, any information available regarding the source of the data.
- Any automated decision United Colleges Group has taken about the individual, together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

19.2 Identifying Relevant Personal Data (Authorised Employees)

19.2.1 The Data Privacy Team is responsible for leading the effort to locate personal data relevant to the DSAR and must identify all departments that might reasonably be considered to hold personal data relevant to the DSAR. For the *UCG Authorised Employees List* see Appendix 2.

19.2.2 The Data Privacy Team will contact and ask the relevant departments for the required information as requested in the DSAR. This may also involve an initial meeting with the relevant departments to go through the DSAR, if required. The department which holds the information must return the required information by the deadline imposed by the Data Privacy Team and/or a further meeting is arranged with the department to review the information.

19.2.3 The Data Privacy Team will determine whether there is any information which may be subject to an exemption and/or if consent is required to be provided from a third party.

19.3 How to Locate Information (Authorised Employees)

19.3.1 The personal data United Colleges Group need to provide in response to a DSAR may be located in several of United Colleges Group's electronic and manual filing systems or on those of United Colleges Group's data processors or other third parties. This is why it is important to identify at the outset the type of information requested so that the search can be focused. For the *UCG Authorised Employees List* see Appendix 2.

19.3.2 The Data Privacy Team will work with the IT department to collect the personal data about the individual from all relevant sources including:

✓	Automated systems such as door entry or key card access systems.
✓	Emails, electronic files and documents, electronic systems, e.g. databases, networked and non-networked computers, servers, computer hard drives, word processing systems, customer records, human resources systems, email data and back up data.
✓	Hard copy files, manual filing systems in which personal data is accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data.
✓	Voice recordings, photographs, monitoring records and CCTV images, internet logs and telephone records.
✓	Third-party data processors' systems, data systems held externally by data processors, e.g. external payroll service providers.
✓	Devices used by employees and others.
✓	Occupational health records.
✓	Pensions data.
✓	Insurance benefit information.
✓	Data held by consultants engaged by United Colleges Group.

19.3.3 The Data Privacy Team should search these systems using the individual's name, employee number, customer account number or other personal identifier as a search determinant.

19.3.4 Employees asked to search for information must carry out the search in full.

19.3.5 The Data Privacy Team will provide guidance and support to employees conducting searches, but it is the responsibility of individual employees to search for and collate the information where possible.

19.3.6 If there are likely to be any issues in conducting the search, employees must notify the Data Privacy Team immediately so that any requirement to extend the time to respond, or apply a fee, can be considered and the requestor notified within the month of receipt of the request.

19.4 Exemptions (DPO Only)

19.4.1 A Data Subject does not have the right to access information recorded about someone else, unless they are an authorised representative, or have parental responsibility.

19.4.2 United Colleges Group is not required to respond to requests for information unless it is provided with enough details to enable the location of the information to be identified, and to satisfy itself as to the identity of the individual making the request.

19.4.3 In certain circumstances United Colleges Group may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

19.5 Exemptions Guidance Table

<p>Information about other people</p>	<p>A DSAR may cover information which relates to an individual or individuals other than the Data Subject.</p> <p>United Colleges Group cannot refuse to provide access to personal data simply because the data refers to a third-party source. Instead, the organisation is required to undertake a ‘balancing act’ to ensure the privacy rights of the Data Subject requesting the data and the third party included in the data are respected.</p> <p>Where the data includes third party information, it may be possible to: anonymise the data relating to the third party; seek consent from the third party; or decide if the disclosure is reasonable, bearing in mind any duty of confidentiality owed to the third party as well as any statutory requirements.</p>
<p>Similar or identical requests</p>	<p>Where a similar or identical request in relation to the same Data Subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that Data Subject, any further request made within a six month period of the original request will be considered a repeat request, and United Colleges Group will not normally provide a further copy of the same data.</p>
<p>Publicly available information</p>	<p>United Colleges Group is not required to provide copies of documents which are already in the public domain.</p>
<p>Privileged documents</p>	<p>Any privileged information held by United Colleges Group need not be disclosed in response to a DSAR. In general, privileged information includes any document which is confidential (e.g. a direct communication between a client and his/her lawyer) and is created for</p>

	the purpose of obtaining or giving legal advice.
Crime detection and prevention	United Colleges Group does not have to disclose any personal data which it is processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. United Colleges Group is still required to provide as much of the personal data as it can. For example, if the disclosure of the personal data could alert the individual to the fact that they are being investigated for an illegal activity (i.e. by United Colleges Group or by the police) then United Colleges Group does not have to disclose the data since the disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.
Corporate finance	United Colleges Group does not have to disclose any personal data which it processes for the purposes of, or in connection with, a corporate finance service if: <ul style="list-style-type: none"> • Disclosing the personal data would be likely to affect the price of an instrument; or • Disclosing the personal data would have a prejudicial effect on the orderly functioning of financial markets or the efficient allocation of capital within the economy and we believe that it could affect a person's decision: <ol style="list-style-type: none"> i. Whether to deal in, subscribe for or issue an instrument. ii. Whether to act in a way likely to have an effect on a business activity, e.g. on the industrial strategy of a person, the capital structure of an undertaking or the legal or beneficial ownership of a business or asset.
Confidential references	United Colleges Group does not have to disclose any confidential references that United Colleges Group has given to third parties for the purpose of actual or prospective: <ul style="list-style-type: none"> • Education, training, or employment of the data subject. • Appointment of the data subject to any office. • Provision by the data subject of any service.
Management forecasting	United Colleges Group does not have to disclose any personal data which it processes for the purposes of management forecasting or management planning to assist United Colleges Group in the conduct of any business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies, succession planning, promotions, and demotions. This exemption must be considered on a case-by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.
Negotiations	United Colleges Group does not have to disclose any personal data consisting of records of its intentions in relation to any negotiations with the data subject, where doing so would be likely to prejudice those negotiations. For example, if the HR department is negotiating with an employee in order to agree the terms of a redundancy package and the

	<p>employee makes a Data Subject Access Request, the HR department can legitimately withhold giving access to information which would prejudice those redundancy negotiations. The HR department must, however, disclose all other personal data relating to the Data Subject unless this other personal data are also exempt from disclosure. Please note that reliance on the negotiation exemption would only apply if negotiations were ongoing.</p>
--	--

20. CORRECTION (RECTIFICATION) REQUESTS

- 20.1 Data Subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a Data Subject providing a supplementary statement regarding the data.
- 20.2 Where a rectification request is made, the Data Privacy Team must rectify the personal data without undue delay unless a basis exists to deny the request.
- 20.3 The Data Privacy Team must identify each third-party recipient of the personal data that is the subject of the rectification request. The Data Privacy Team must communicate the rectification of the personal data to each recipient (for example, United Colleges Group third-party service providers who process the data on our behalf), unless the Data Privacy Team issues a written finding that it is impossible or involves disproportionate effort. The Data Privacy Team must also inform the Data Subject about those recipients if the Data Subject requests it.
- 20.4 The Data Privacy Team must determine if United Colleges Group have a basis not to respond to the rectification request. The Data Privacy Team must inform the data subject of the reason for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

21. ERASURE REQUESTS

- 21.1 Data Subjects have the right, in certain circumstances, to have United Colleges Group erase their personal data. Where such a request is made, the Data Privacy Team must, unless an exemption applies, erase the personal data that is the subject of the request if:
- The personal data is no longer necessary for the purpose United Colleges Group collected it for.
 - The Data Subject withdrew their consent to our processing activities and no other legal justification for processing applies.
 - The Data Subject objects to:
 - (i) Processing, including profiling, which is necessary for United Colleges Group to perform a task in the public interest or in the exercise of our official authority; and
 - (ii) There are no overriding legitimate grounds to process the personal data.
 - The Data Subject objects under GDPR Article 21(1) to:
 - (i) Processing, including profiling, which is necessary to pursue United Colleges Group's or a third party's legitimate interest; and
 - (ii) There are no overriding legitimate grounds to process the personal data.

- The Data Subject objects to processing for direct marketing purposes.
 - United Colleges Group unlawfully processed the Data Subject's personal data.
 - EU or member state law requires United Colleges Group to erase the personal data to comply with a legal obligation.
 - United Colleges Group collected the personal data in the context of offering online services to children by obtaining consent.
- 21.2 If United Colleges Group determines that it must erase the Data Subject's data in response to the request, and it made the personal data that is the subject of the erasure request public, the Data Privacy Team must take reasonable steps, including technical measures, to inform other organisations processing the personal data of the erasure request, including removing any links to, and copies of, the personal data.
- 21.3 If United Colleges Group determines that it must erase the Data Subject's data in response to the request, the Data Privacy Team must identify each recipient to whom it disclosed the personal data that is the subject of the erasure request. The Data Privacy Team must communicate the erasure of personal data to the third-party data recipients, unless the Data Privacy Team issues a written finding that this is impossible or involves disproportionate effort. The Data Privacy Team must also notify the Data Subject about those recipients if they request that information.
- 21.4 In addition to the general grounds for denying a data subject request, United Colleges Group may also refuse to respond to a Data Subject erasure request if it processes personal data that is necessary for:
- 21.4.1 Exercising the right of freedom of expression and information.
 - 21.4.2 Complying with a legal obligation under EU or member state law.
 - 21.4.3 The performance of a task carried out in the public interest.
 - 21.4.4 Public health reasons consistent with the exceptions for processing sensitive personal data such as health information, as outlined in GDPR Articles 9(2)(h) and (i) and 9(3).
 - 21.4.5 Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes under Article 89(1), if the erasure is likely to render impossible or seriously impair the processing objectives.
 - 21.4.6 The establishment, exercise, or defence of legal claims.
- 21.5.1 The Data Privacy Team must determine if United Colleges Group has a basis not to respond to a Data Subject erasure request. The Data Privacy Team must inform the Data Subject of the reasons for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

22. REQUESTS TO RESTRICT PERSONAL DATA PROCESSING

- 22.1 Data Subjects have the right, in certain circumstances, to request that United Colleges Group restrict the processing of their personal data. Where such a request is made, the Data Privacy Team must, unless an exemption applies, restrict processing of the Data Subject's personal data if:
- 22.1.1 The Data Subject contests the accuracy of the personal data. United Colleges Group must restrict processing the contested data until it can verify its accuracy.
 - 22.1.2 The processing is unlawful. Instead of requesting erasure of the data the Data Subject can request that United Colleges Group restrict use of the unlawfully processed personal data.

22.1.3 United Colleges Group no longer needs to process the personal data, but the Data Subject needs the personal data for the establishment, exercise, or defence of legal claims.

22.1.4 A Data Subject objects to processing, including profiling, for:

- (i) Purposes that United Colleges Group consider necessary to perform a task in the public interest; or
- (ii) Purposes that United Colleges Group consider necessary for its or a third party's legitimate interest.

22.2 If the Data Subject objects to processing, United Colleges Group must restrict the challenged processing activity pending verification of whether it's or a third party's legitimate interests override the Data Subject's interests.

22.3 The Data Privacy Team must determine if United Colleges Group has a basis not to respond to the data processing restriction request. The Data Privacy Team must inform the Data Subject of the reason for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

22.4 Where processing has been restricted, the Data Privacy Team must ensure that United Colleges Group only process the personal data (excluding storing it) either:

- With the Data Subject's consent.
- For the establishment, exercise, or defence of legal claims.
- For the protection of the rights of another person.
- For reasons of important public interest.

22.5 The Data Privacy Team must inform the Data Subject that United Colleges Group intends to lift the restriction 5 days before lifting the restriction. United Colleges Group may lift the processing restriction when:

- The Data Privacy Team verifies the accuracy of the personal data that is the subject of the processing restriction request.
- The Data Privacy Team determines that the college's or a third party's legitimate interests override the Data Subject's interests if a Data Subject objects on the grounds outlined above.

22.6 Where processing has been restricted, the Data Privacy Team must identify each recipient to whom United Colleges Group disclosed the personal data that is the subject of the processing restriction request. The Data Privacy Team must communicate the processing restriction to the third-party data recipients, unless the Data Privacy Team issues a written finding that it is impossible or involves disproportionate effort. The Data Privacy Team must also notify the Data Subjects about those recipients if they request that information.

23. DATA PORTABILITY REQUESTS

23.1 Data Subjects have the right, in certain circumstances, to:

- Receive a copy of certain personal data from United Colleges Group in a structured, commonly used, and machine-readable format and store it for further personal use on a private device.
- Transmit certain personal data to another data controller.
- Have United Colleges Group transmit certain personal data directly to another data

controller, where technically possible.

- 23.2 The data portability right only applies to personal data processed by automated means when processing is either:
- Based on the Data Subject's consent.
 - Necessary to perform a contract with the Data Subject.
- 23.3 The personal data covered by the data portability right includes only personal data concerning the Data Subject which the Data Subject knowingly and actively provided to United Colleges Group such as name, contact information, and browsing history. The data portability right does not include data that United Colleges Group creates from the data provided by the Data Subject such as a user profile. If you have any questions about whether personal data falls within the scope of a data subject portability request, please contact the Data Privacy Team.
- 23.4 For personal data that the Data Subject requests be transmitted to a third party the Data Privacy Team must, unless an exemption applies, transfer the personal data that is the subject of the data portability request in any of the following formats: email, letter and telephone.
- 23.5 If the Data Subject requests a particular format the Data Privacy Team should make efforts to transfer the data in that format.
- 23.6 For portability requests asking that the personal data be transmitted directly to the Data Subject, the Data Privacy Team must, unless an exemption applies, transfer the personal data that is the subject of the data portability request.
- 23.7 If the Data Subject requests a particular format, the Data Privacy Team should make efforts to transfer the data in that format.
- 23.8 Personal Data Pertaining to Third Parties:
- Where the data set includes third parties' personal data United Colleges Group must identify a legal basis under Data Protection Law prior to transferring the third parties' data. The Data Privacy Team must determine whether United Colleges Group has a basis to transfer the third parties' data.
 - In cases where the Data Privacy Team determines that United Colleges Group does not have a basis to transfer the personal data of third parties, the Data Privacy Team may give instructions to redact or remove the personal data of the third parties prior to transmitting the data in response to a portability request.
- 23.9 In addition to the general grounds for denying a Data Subject Request, United Colleges Group may also refuse to respond to a Data Subject portability request if responding to the request adversely affects the rights and freedoms of others.
- 23.10 The Data Privacy Team must determine if United Colleges Group has a basis not to respond to a data portability request. The Data Privacy Team must inform the Data Subject of the reason for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

24. OBJECTIONS TO PERSONAL DATA PROCESSING

- 24.1 Data Subjects have the right to object to personal data processing when United Colleges

Group process their personal data:

- For direct marketing purposes, including profiling related to direct marketing. United Colleges Group must stop processing a Data Subject's personal data for direct marketing purposes whenever the Data Subject objects.
- For scientific or historical research purposes or statistical purposes, subject to the exceptions as described.
- For a task carried out in the public interest or the exercise of official authority vested in United Colleges Group.
- For the legitimate interests of us or a third party.

24.2 The Data Privacy Team must, unless an exemption applies, stop the personal data processing related to the Data Subject's request.

24.3 In addition to the general grounds for denying a Data Subject Request, United Colleges Group can refuse to grant a Data Subject processing objection when:

- A Data Subject objects to processing for scientific or historical research purposes or statistical purposes and United Colleges Group demonstrates that the processing is necessary for United Colleges Group to perform a task in the public interest.
- A Data Subject objects to processing, including profiling, for processing for a task carried out in the public interest or the exercise of official authority vested in United Colleges Group; or for processing necessary for the legitimate interests of United Colleges Group or a third party; and United Colleges Group demonstrates a compelling legitimate ground for processing the personal data that overrides the Data Subject's interests; or that United Colleges Group needs to process the personal data to establish, exercise, or defend legal claims.

24.4 For objections to data processing, United Colleges Group must temporarily restrict processing of that personal data in accordance with this policy pending verification of whether United Colleges Group legitimate interests override those of the Data Subject.

24.5 If the Data Privacy Team determines that there are no overriding legitimate grounds for the personal data processing as outlined above, the Data Privacy Team must erase that personal data in accordance with the terms of this policy.

24.6 The Data Privacy Team must determine if United Colleges Group has a basis not to respond to a Data Subject objection request. The Data Privacy Team must inform the Data Subject of the reasons for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

25. AUTOMATED DECISION-MAKING OBJECTIONS

25.1 Data Subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, including profiling, if the decision produces legal or other similarly significant effects on them.

25.2 The Data Privacy Team must determine if the automated decision-making, including profiling, produces legal effects on the Data Subject or affects them in a similarly significant way.

25.3 The Data Privacy Team must, unless an exemption applies, stop the automated decision-making that is the subject of the Data Subject Request.

25.4 In addition to the general grounds for denying a Data Subject Request set out above, United Colleges Group can refuse to grant an automated decision-making objection when the automated decision is either:

- Necessary for entering into or performing a contract with the Data Subject.
- Authorized by UK applicable law to United Colleges Group.
- Based on the Data Subject’s explicit consent.

25.5 The Data Privacy Team must determine if United Colleges Group has a basis not to respond to the Data Subject’s automated decision-making objection. The Data Privacy Team must inform the Data Subject of the reasons for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

26. RECORDS MANAGEMENT FOR THIS PROCEDURE

Record name	Storage location	Team responsible	Controls for record protection	Retention time
Data Subject Access Request Forms	ISMS/Applied Controls/A18 Legal & Compliance/Data Privacy/Managing Data Subject Access Requests	Data Privacy Team	Only authorized persons may access the folder	6 months following the last correspondence with the Data Subject relating to that Data Subject Request
Data Subject Disclosure Form	ISMS/Applied Controls/A18 Legal & Compliance/Data Privacy/Managing Data Subject Access Requests	Data Privacy Team	Only authorized persons may access the folder	6 months following the last correspondence with the Data Subject relating to that Data Subject Request

The Data Privacy Team must delete or destroy all identification and proof of legal authority documentation 6 months after confirmation of the third-party’s identity and legal authority to act on the Data Subject’s behalf.

27. CONSEQUENCES OF FAILING TO COMPLY WITH THIS POLICY (ALL EMPLOYEES)

27.1 If United Colleges Group fails to comply with a Data Subject Request or fails to respond within a 30-day period, United Colleges Group will be in breach of Data Protection Law. This may have several consequences:

- It may put at risk the Data Subject whose personal information is being processed.

- The Data Subject may complain to the ICO. This may lead the ICO to investigate the complaint. If United Colleges Group is found to be in breach, enforcement action could follow, which carries the risk of significant civil and criminal sanctions for United Colleges Group and, in some circumstances, for the individual responsible for the breach.
- If a Data Subject has suffered damage, or damage and distress, because of United College Group’s breach of Data Protection Law or other relevant legislation, the Data Subject may take United Colleges Group to court and claim damages from United Colleges Group.
- A court may order United Colleges Group to comply with the Data Subject Request if United Colleges Group is found not to have complied with its obligations under the GDPR and other relevant legislation.

27.2 Violation of this policy may result in disciplinary action which may include termination of staff and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of United Colleges Group information resources access privileges, civil, and criminal prosecution.

27.3 Any exception to the policy must be approved by the Data Privacy Team in advance.

28. COMPLIANCE MEASUREMENT

The Data Privacy Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Appendix 1

UCG Data Subject Access Request Form

1.0 DATA SUBJECT DETAILS:

Title	Mr <input type="checkbox"/>	Mrs <input type="checkbox"/>	Miss <input type="checkbox"/>	Ms <input type="checkbox"/>	Other: <input type="checkbox"/>
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					
Date of birth					
Details of identification provided to confirm name of data subject:					

Details of data requested:	
----------------------------	--

1.1 DETAILS OF PERSON REQUESTING THE INFORMATION (if not the Data Subject):

Are you acting on behalf of the data subject with their written or other legal authority?	Yes <input type="checkbox"/>				
	No <input type="checkbox"/>				
If 'Yes' please state your relationship with the data subject (e.g., parent, legal guardian, or solicitor)					
Please enclose proof that you are legally authorised to obtain this information.					
Title	Mr <input type="checkbox"/>	Mrs <input type="checkbox"/>	Miss <input type="checkbox"/>	Ms <input type="checkbox"/>	Other: <input type="checkbox"/>
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					

2. DECLARATION

I,, the undersigned and the person identified in (1) above, hereby request that UCG provide me with the data about me identified above.

Signature:

Date:

DSAR form completed by (Staff/Student name):

I,, the undersigned and the person identified in (1.1) above, hereby request that UCG provide me with the data about the data subject identified in (1) above.

Signature:

Date:

DSAR form completed by (name):

This form must immediately be forwarded to the Data Protection Team: gdpr@ucg.co.uk

Appendix 2

UCG Authorised Employees List

General Data Subject Access Requests

Data Privacy Team: gdpr@ucg.ac.uk

GRCI Law (DPO): dpoas@grcilaw.com

Gora Selliah: gora.selliah@cw.ac.uk

Iqbal Khan: iqbal.khan@cw.ac.uk

Education Reference Requests

Wendy Hall: wendy.hall@cw.ac.uk

CNWL Enquiries: enquiries@cnwl.ac.uk

Marta Lupikasza: marta.lupikasza@cnwl.ac.uk