UNIVERSITY OF CAMBRIDGE

COUNCIL

UPDATE ON PREPARATIONS FOR THE GENERAL DATA PROTECTION REGULATION

Purpose

This paper is designed to:

(a) update the Council about the University's preparations for the General Data Protection Regulation (GDPR), which will apply from 25 May 2018;

(b) seek the Council's approval of the draft new Data Protection Policy for the University; and

(c) seek the Council's approval, for the University's part, of the draft new Data Sharing Protocol between the University, the 31 Colleges and Cambridge in America.

Executive summary

External developments

- The GDPR, as a European Regulation, will apply in the UK and across the EU from 25 May 2018.
- The UK Data Protection Bill, which supplements the GDPR in various ways, is proceeding through Parliament and will need to receive Royal Assent by the same date. The supplementary provisions in the Bill largely are helpful and the University has been instrumental in lobbying around some of these.
- As well as the new legislation, significant volumes of guidance have been published at both national and European level.

Internal developments

- The University's preparations, overseen by the GDPR Data Protection Working Group, generally are proceeding to timetable and plan.
- Many of the necessary changes are being implemented centrally in the following broad areas:
    - The establishment of new policies and template documents.
    - The implementation of new data sharing protocols and agreements with third parties.
    - The appointment of a new statutory Data Protection Officer role.
    - The publication of new core privacy notices aimed at different types of individual, and associated changes to documentation issued during numerous processes to applicants, students, staff, alumni and others.
    - The development of an Information Asset Register.

- The completion of GDPR and security checklists for major IT systems and associated remedial action.
- The creation of new training courses and materials.

- Extensive guidance and communications are being published and circulated to Institutions for them to implement their local preparations.
- Deloitte LLP, the University's internal auditors, reviewed the University's preparations in October 2017. Their report noted the wide scope of the University's plans, commended the progress made in various areas and made recommendations – which are being implemented – for some further work.

Documents for approval

- The draft new Data Protection Policy and the draft new Data Sharing Protocol between the University, the 31 Colleges and Cambridge in America are annexed for the Council's approval.

Introduction

1. A briefing paper on the GDPR and the University's preparations was presented to the 24 April 2017 meeting of the Council (Agenda B3; Minute 101).[1] This update paper summarises external and internal developments since that date, and seeks the Council's approval of two core documents.

External developments

2. As a European Regulation, the GDPR applies in full in all EU Member States from 25 May 2018 and sets out enhanced provisions for the handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects') by organisations ('data controllers'). The GDPR, however, permits individual EU Member States to derogate from (i.e. amend) the standard provisions in certain areas. The Department for Digital, Culture, Media and Sport (DCMS), as the responsible UK Government department, launched its consultation exercise on the derogations in April 2017. The University responded in its own right, as well as contributing to sector-wide responses by Universities UK, the Russell Group and the Council for the Advancement and Support of Education (CASE). Like many respondents, including those from the Higher Education sector, the University advocated the continuation of the existing exemptions within the Data Protection Act 1998 wherever possible. It also sought a clear definition in UK law of a 'public authority' for GDPR purposes and argued that the sector should be excluded from that definition. The University also continued its lobbying efforts with the DCMS and the ICO on this point.

[1] The paper is at https://www.governance.cam.ac.uk/committees/council/meeting-20170424/CategoryBDocuments/B3%20General%20Data%20Protection%20Regulation.pdf and the Minutes are at https://www.governance.cam.ac.uk/committees/council/meeting-20170424/MeetingDocuments/Council_confirmed%20minutes%2024%20Apr%2017.pdf.

3. The Data Protection Bill was introduced in the House of Lords in September 2017. As well as enacting the derogations in the UK, the Bill delineates the regulatory role and powers of the Information Commissioner's Office and implements associated legislation. The first draft of the Bill contained many of the derogations sought by that the University in its consultation response, but it defined a GDPR public authority by reference to all bodies subject to the Freedom of Information Act 2000 (including universities). Further lobbying, in which the University was instrumental, has achieved a useful narrowing of the definition such that public authority status for GDPR purposes is limited to those times when an organisation is exercising its public functions or official authority. (In practical terms the most significant impact of this is that the University can continue to rely on the 'legitimate interests' legal basis for processing personal data – which otherwise is unavailable for public authorities – for all of its non-public functions.) The Bill was passed in the House of Lords in January 2018 and is now proceeding through the House of Commons so as to achieve Royal Assent and apply alongside the GDPR from May 2018.

4. The ICO and the Article 29 Working Party (the collective group of European data protection regulators) both have issued various pieces of GDPR guidance, of greater or lesser relevance to the Higher Education sector, and the University has kept abreast of these insofar as they impact upon its preparations.

5. The proposed European Regulation on Privacy and Electronic Communications, which was published in January 2017 and had been scheduled to apply alongside the GDPR from 25 May 2018, has been delayed and no timetable has been set for its implementation. The proposed Regulation supplements the GDPR in specific areas such as the rules on direct electronic marketing communications and website cookies banners.

Internal developments

6. The University's GDPR Data Protection Working Group, established in summer 2016, has continued to oversee the University's preparations. Chaired by the Registrary, it has met eight times to date. Its principal activity, as well as keeping abreast of external developments, has been the general oversight of progress against the University's GDPR Implementation Project Plan though it has also scrutinised certain core documentation. The Joint Committee on Development's ad-hoc Working Group on Fundraising-related Regulations also has continued to meet to discuss specific changes with regard to alumni and supporter data processing arising from the GDPR. The Colleges, Cambridge Assessment and Cambridge University Press, who are all represented on the University's Working Group, have continued to make separate but parallel (and often integrated) preparations.

7. The principal actions from the GDPR Implementation Project Plan which have been completed or are underway are as follows:

   (a) A new Data Protection Policy for the University has been drafted (see paragraph 9 below).

(b) A new Data Sharing Protocol between the University, the 31 Colleges and Cambridge in America has been drafted (see paragraph 10 below).

(c) New template agreements and clauses for data sharing with other third party organisations (whether other data controllers using data for their own purposes or data processors using personal data solely on the University's behalf) have been created and existing contracts are being reviewed and revised wherever possible.

(d) The scope of the new statutory Data Protection Officer role for the University Group has been defined. The proposal is to outsource the appointment on a part-time service contract basis in the first instance. This will achieve the necessary seniority, independence and expertise for the role and will allow for future flexibility while we obtain a better understanding for how the role will operate in practice. A procurement process is underway.

(e) A systematic re-assessment of the appropriate lawful basis for the use of the personal data of many types of data subject in different ways has been carried out. New core privacy notices have been published to explain to various types of data subject (e.g. applicants, students, alumni, staff) the uses made of their personal data. Numerous forms, portals and websites have been amended to reflect the updated provisions (often removing consent mechanisms that were inappropriate).

(f) A formal project has been initiated within UIS to create an Information Asset Register (IAR) to hold records of data processing activities across the University. The main users will be Departmental Administrators (and equivalents), a group of which has been involved in piloting and testing the system. The IAR will be launched shortly.

(g) Checklists have been developed and completed to enable the systematic assessment of major IT systems against the GDPR's security requirements and wider provisions. Remediation work is underway as necessary. Procedures for responding to and logging personal data breaches and data subject rights requests are being updated and tested.

(h) The redrafting of the University's Information Data Security Policy, and its associated sub-policies and procedures, is ongoing. Procedures for embedding privacy by design principles into IT projects, and a template for conducting a full Data Protection Impact Assessment, have been drafted and are being finalised.

(i) New guidance for researchers is being created. The exemptions from the GDPR for research (which principally are contained in the Data Protection Bill) are complex and apply in different ways depending on the nature of the research. Proposals have been developed for the integration of light-touch Data Protection Impact Assessments into existing research ethics committee processes.

(j) A new online data protection training module for staff has been written and is being tested. It will be launched shortly.

(k) An extensive toolkit of guidance for University Institutions has been prepared and was circulated to all departments in November 2017. The toolkit explains the GDPR and contains highly practical guidance for local preparations to supplement those that can be made centrally. A number of workshops were held in December 2017 to help Departmental Administrators (and others) to use the toolkit, and a programme of follow-up communications is underway. Both the Toolkit and the workshops have been well received.

(l) General online guidance on data protection and the GDPR has been and will continue to be rewritten. A dedicated GDPR page was created in June 2017 and has been regularly updated.[2] Numerous presentations and briefings have been given to different audiences across the University (and to related organisations such as the student unions and the related Trusts).

(m) Numerous consequential changes – for example to HR processes/forms or to the procedures for the public display of class-lists – have been implemented or are underway.

8. Deloitte LLP, the University's internal auditors, reviewed the University's GDPR preparations in October 2017. Their final report (issued in February 2018 and presented to the March 2018 meeting of the Audit Committee)[3] noted the wide scope of the University's GDPR Implementation Project Plan and the progress made in various areas, but made a number of recommendations for further work, including a plan for transition to business as usual. Work is underway to address these recommendations alongside the delivery of the remainder of the actions in the Project Plan by 25 May 2018.

Documents for approval

9. Annex 1 contains the draft new Data Protection Policy for the University for the Council's approval (on the recommendation of the GDPR Data Protection Working Group). The University has not hitherto had a policy in this area but it is a clear expectation of the GDPR that any large organisation will have such a policy as part of its accountability obligations. The policy was drafted by the Information Compliance Officer and includes extensive input from members of the Working Group, including the Chief Information Security Officer and the member from the Legal Services Office.

---

[2] See https://www.information-compliance.admin.cam.ac.uk/data-protection/general-data-protection-regulation.

[3] At its meeting on 8 March 2018, the Audit Committee noted: that the University had begun its preparations for GDPR promptly and that substantial progress had been made to date; that complications had arisen from the devolved nature of the University; that, like many large and complex organisations, it was a significant challenge for the University to achieve and evidence enhanced levels of compliance in every area by 25 May 2018; and that the DPO appointment, amongst other matters, still required resolution.

10. Annex 2 contains the draft new Data Sharing Protocol between the University, the 31 Colleges and Cambridge in America for the Council's approval (on the recommendation of the GDPR Data Protection Working Group). This new protocol would replace the two existing separate protocols between the University and the 31 Colleges for the sharing of student and alumni personal data, as well as the existing separate protocol between the University and Cambridge in America for the sharing of alumni personal data. The draft new Data Sharing Protocol between the University, the 31 Colleges and Cambridge in America has been approved by the Colleges' Committee (at its meeting on 24 February 2018) on behalf of the Colleges and approval is being sought from the CAm Board on behalf of Cambridge in America.

Conclusion

11. The Council is asked to:

    (a) note this update paper;

    (b) approve the draft new Data Protection Policy for the University (as set out in Annex 1); and

    (c) approve, for the University's part, the draft new Data Sharing Protocol between the University, the 31 Colleges and Cambridge in America (as set out in Annex 2).

Dr James Knapton
Information Compliance Officer
Registrary's Office
9 March 2018

ANNEX 1

University of Cambridge

Data Protection Policy

1 Purpose and scope

1.1 The purpose of this policy is to ensure compliance with the General Data Protection Regulation and related EU and national legislation ('data protection law').[1] Data protection law applies to the storing or handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects').

1.2 This policy applies to all parts of the University of Cambridge ('the University'), as a single organisation ('data controller'), with the exception of Cambridge Assessment and Cambridge University Press.[2] It does not apply to the Colleges, associated Trusts or subsidiary companies, which are separate legal entities and data controllers.

1.3 This policy applies to all staff except when acting in a private or non-University capacity. In this policy, the term 'staff' means anyone working in any context within the University at whatever level or grade and whether permanent, fixed term or temporary, including but not limited to employees, retired but active research staff, other visiting research or teaching staff, workers, trainees, interns, seconded staff, agency staff, agents, volunteers, and external members of committees.

1.4 This policy applies to all students when processing personal data on behalf of the University, but not in any other situation including when acting in a private or non-University capacity.

1.5 This policy is not, and should not be confused with, a privacy notice (a statement informing data subjects how their personal data is used by the University).[3]

1.6 This policy should be read in conjunction with the obligations in the following documents, which supplement this policy where applicable:

1.6.1 staff employment contracts and comparable documents (e.g. worker agreements), which impose confidentiality obligations in respect of information held by the University;[4]

1.6.2 information security policies, procedures and terms and conditions, which concern the confidentiality, integrity and availability of University information, and which include rules about acceptable use, breach reporting, IT monitoring, and the use of personal mobile devices;[5]

---

[1] See http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[2] Cambridge Assessment and Cambridge University Press have their own data protection policies.

[3] For which see https://www.information-compliance.admin.cam.ac.uk/data-protection/general-data and other notices (including those on related webpages).

[4] See https://www.hr.admin.cam.ac.uk/recruitment-guidance.

[5] See https://www.uis.cam.ac.uk/about-us/governance/information-services-committee/rules-and-guidelines and related webpages.

1.6.3 records management policies and guidance, which govern the appropriate retention and destruction of University information;[6] and

1.6.4 any other contractual obligations on the University or individual staff which impose confidentiality or data management obligations in respect of information held by the University, which may at times exceed the obligations of this and/or other policies in specific ways (e.g. in relation to storage or security requirements for funded research).

2 Policy statement

2.1 The University is committed to complying with data protection law as part of everyday working practices.

2.2 Complying with data protection law may be summarised as but is not limited to:

2.2.1 understanding, and applying as necessary, the data protection principles when processing personal data;[7]

2.2.2 understanding, and fulfilling as necessary, the rights given to data subjects under data protection law;[8] and

2.2.3 understanding, and implementing as necessary, the University's accountability obligations under data protection law.[9]

3 Roles and responsibilities

3.1 The University has a corporate responsibility as a data controller (or when acting as a joint data controller or a data processor) for:

3.1.1 complying with data protection law and holding records demonstrating this;

3.1.2 cooperating with the Information Commissioner's Office (ICO) as the UK regulator of data protection law; and

---

[6] See https://www.information-compliance.admin.cam.ac.uk/records-management.

[7] The principles in relation to personal data are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

[8] The data subject rights are: to be informed; access; rectification; erasure; restriction; data portability; and objection (including in relation to automated decision-making).

[9] The accountability obligations include: implementing appropriate data protection policies; implementing data protection by design and default in projects, procurement and systems; using appropriate contracts with third party data controllers and data processors; holding relevant records about personal data processing; implementing appropriate technical and organisational security measures to protect personal data; reporting certain personal data breaches to the Information Commissioner's Office; conducting Data Protection Impact Assessments where required; and ensuring adequate levels of protection when transferring personal data outside the European Economic Area.

3.1.3 responding to regulatory/court action and paying administrative levies and fines issued by the ICO.

3.2 The University Council is responsible for:

3.2.1 reviewing (at least once every five years) and approving this policy; and

3.2.2 assessing the overall risk profile and ensuring appropriate resources and processes are in place and implemented to enable compliance with data protection law.

3.3 The independent University Data Protection Officer is responsible for:

3.3.1 monitoring and auditing the University's compliance with data protection law, especially its overall risk profile, and reporting annually to the University Council;

3.3.2 advising the University, usually through its Information Compliance Office,[10] on all aspects of its compliance with data protection law (including its use of Data Protection Impact Assessments);

3.3.3 acting as the University's standard point of contact with the ICO with regard to data protection law, including in the case of personal data breaches; and

3.3.4 acting as an available point of contact for complaints from data subjects.

3.4 The Information Compliance Office, in collaboration with other relevant offices, is responsible for:

3.4.1 providing advice, guidance, training and tools/methods, in accordance with the University's overall risk profile and having taken into account the advice of the independent Data Protection Officer, relevant case law and ICO/other regulatory guidance, to help University Institutions and staff comply with this policy;

3.4.2 publishing and maintaining core privacy notices and other University-wide data protection documents;

3.4.3 handling data subject rights requests; and

3.4.4 as advised by the University Data Protection Officer, managing and/or handling Data Protection Impact Assessments, data subject complaints and personal data breaches.

3.5 Heads of Institutions are responsible for:

[10] Within the Registrary's Office (a Division of the Unified Administrative Service).

3.5.1 making all staff within their Institution aware of this policy as necessary;

3.5.2 ensuring that appropriate processes and training are implemented within their Institution to enable compliance with data protection law; and

3.5.3 ensuring that appropriate processes are implemented within their Institution to enable information assets containing personal data within their Institution to be included in the University's Information Asset Register.

3.6 Individual staff, as appropriate for their role and in order to enable the University to comply with data protection law, are responsible for:

3.6.1 completing relevant data protection training;

3.6.2 following relevant advice, guidance and tools/methods provided by the Information Compliance Office (and other relevant offices) depending on their role, regardless of whether access to and processing of personal data is through University-owned and managed systems, or through their own or a third party's systems and devices;

3.6.3 when processing personal data on behalf of the University, only using it as necessary for their contractual duties and/or other University roles and not disclosing it unnecessarily or inappropriately;

3.6.4 recognising, reporting internally, and cooperating with any remedial work arising from personal data breaches;

3.6.5 recognising, reporting internally, and cooperating with the fulfilment of data subject rights requests;

3.6.6 when engaging with students who are using personal data in their studies and research, advising those students of relevant advice, guidance and tools/methods to enable them to handle such personal data in accordance with this policy; and

3.6.7 only deleting, copying or removing personal data when leaving the University as agreed with their Head of Institution and as appropriate.

3.7 The responsibilities in paragraph 3.6 apply to individual students when processing personal data on behalf of the University.

3.8 Non-observance of the responsibilities in paragraph 3.6 may result in disciplinary action.

3.9 The roles and responsibilities in paragraphs 3.1 to 3.8 do not waive any personal liability for individual criminal offences for the wilful misuse of personal data under data protection law.[11]

4 Contact and date of last revision

4.1 Contact details are published on the Information Compliance Office's webpages.[12]

4.2 This policy was last revised and approved by the University Council in [March 2018].

[11] These criminal offences include: unlawfully obtaining, disclosing or retaining personal data; recklessly re-identifying de-identified personal data without the data controller's consent; deliberately altering or deleting personal data to prevent disclosure in accordance with data subject access rights; forcing a data subject to exercise their access rights; and knowingly giving false statements to the ICO.

[12] See https://www.information-compliance.admin.cam.ac.uk/contact-us.

ANNEX 2

UNIVERSITY OF CAMBRIDGE

DATED 2018

THE UNIVERSITY, CAMBRIDGE IN AMERICA AND THE COLLEGES

DATA SHARING PROTOCOL

THIS PROTOCOL is dated [DATE] 2018

BETWEEN

(1) The Chancellor, Masters, and Scholars of the University of Cambridge of The Old Schools, Trinity Lane, Cambridge, CB2 1TN (**University**).

(2) Cambridge in America of 1120 Avenue of the Americas, 17th Floor, New York, New York, 10036 (**CAm**).

(3) The 31 Cambridge Colleges as stated in Statute G of the Statutes and Ordinances of the University of Cambridge, contacted collectively through the Office of Intercollegiate Services Ltd., 12B King's Parade, Cambridge, CB2 1SJ (**Colleges**).

BACKGROUND

(A) The University, CAm and the Colleges (the **parties**) work closely together as a collegiate university in relation to fundraising, student affairs and other matters. In relation to this Protocol, the University, the Colleges and CAm act through, or under the authority of, the University Council, Colleges' Committee and the CAm Board respectively.

(B) This Protocol sets out the responsibilities of each of the parties above in areas relating to the protection, security, sharing and processing of Personal Data that two or more of the parties require in order to conduct their individual or shared objectives and activities.

(C) This Protocol replaces the previous data sharing protocols between the parties and is intended to document compliance with the General Data Protection Regulation ((EU) 2016/679) (GDPR). It does not address other commercial or operational issues.

IT IS AGREED AS FOLLOWS:

INTERPRETATION

1 The following definitions apply in this Protocol:

Agreed Purposes: has the meaning given to it in clause 5 of this Protocol.

Data Protection Authority: a national authority, as defined in the GDPR: for the UK, this is the Information Commissioner's Office.

Data Protection Legislation: the General Data Protection Regulation ((EU) 2016/679) (**GDPR**) and any applicable national legislation protecting Personal Data.

Data Security Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

Shared Personal Data: the Personal Data shared between the parties under clause 10 of this Protocol.

Subject Access Request: has the same meaning as "Right of access by the data subject" in Article 15 of the GDPR.

2 **Data Controller**, **Joint Controllers**, **Data Processor**, **Data Subject** and **Personal Data**, **Sensitive Personal Data** or **Special Category Personal Data**, **processing** and **appropriate technical and organisational measures** shall have the meanings given to them in the applicable Data Protection Legislation.

PURPOSE

3 This Protocol sets out the framework for the sharing of Personal Data between the parties as Data Controllers, Joint Controllers and as Data Processors.

4 The parties consider this data sharing necessary and in their mutual best interests as a collegiate university. The aim of the data sharing is to ensure that each party's personal data records, admissions processes, academic processes, employment and membership processes, administration, alumni and supporter relations, and fundraising activities, amongst others, are carried out in a co-ordinated and efficient way.

5 The parties agree to process Shared Personal Data, as described in clause 10, only for and compatible with the following **Agreed Purposes**:

(a) Maintaining academic and teaching records
(b) Administering admissions processes and records
(c) Staff administration and record-keeping
(d) Pursuing alumni and supporter relations, and fundraising activities
(e) Operating communications and IT infrastructure
(f) Marketing
(g) Providing services to staff, students and others
(h) Managing complaints, academic appeals, and disciplinary investigations, where the incident or substance requires input from one or more party
(i) Any other purpose incidental to or analogous with any of the above.

6 Each party shall appoint a single point of contact (SPoC) who will work together to resolve any issues about and improve the effectiveness of the parties' data sharing. A list of the current SPoCs, their names, roles and contact details, shall be maintained by the University's Data Protection Officer and each party commits to updating this information as necessary.

7 Any notice or other formal communication given to a party under or in connection with this Protocol shall be in writing, addressed to the SPoCs and shall be:

(a) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office; or
(b) sent by email to the SPoC.

COMPLIANCE WITH APPLICABLE DATA PROTECTION LEGISLATION

8 Each party must ensure compliance with applicable Data Protection Legislation at all times, including the principles and standards set out in Schedule 1.

9 If the law of New York State imposes different obligations for data processing, CAm shall apply those also but without lessening their compliance with this Protocol.

SHARED PERSONAL DATA

10 The following types of Personal Data may be shared between the parties:

(a) Contact and biographical details
(b) Application, student and alumni records
(c) Staff records
(d) Financial records and details of giving to the University and Colleges
(e) Records relating to alumni and supporter relations, and fundraising
(f) Records relating to the use of services

11 Special Category Personal Data and Sensitive Personal Data may be shared between the parties only where compatible with the Data Protection Legislation.

12 The processing of Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.

13 The parties agree wherever practicable to operate proportionate checks to ensure the accuracy of the Shared Personal Data and its correct incorporation into different systems.

DATA PROCESSING

14 In most cases, the data sharing is such that each party is a separate Data Controller, or are Joint Controllers, of the Shared Personal Data. For specific processing where one party acts only as the Data Processor for another (the Data Controller), the Data Processor shall ensure that it abides by the model data processor clauses issued by the University to comply with Article 28 of the GDPR and published on its website.

DIRECT MARKETING

15 If a party processes the Shared Personal Data for the purposes of direct marketing, that party shall ensure that:

(a) effective procedures and communications are in place to allow the Data Subject to exercise their right to opt out from direct marketing;
(b) effective procedures are in place to enable that party to advise other parties of any opt out that encompasses those other parties; and
(c) an appropriate legal basis has been confirmed (and, where necessary, evidenced) for the Shared Personal Data to be used for the purposes of direct marketing.

DATA SECURITY BREACHES AND REPORTING PROCEDURES

16 The parties agree to provide reasonable assistance to each other to facilitate the handling of any Data Security Breach in an expeditious and compliant manner.

17 The parties should notify any relevant potential or actual losses of the Shared Personal Data and remedial steps taken, either through mechanisms specified by the parties from time to time or otherwise to each and every relevant SPoC as soon as possible, to enable the parties to consider what further action is required either individually or jointly.

REVIEW AND TERMINATION OF PROTOCOL

18 The nature of the arrangements between the parties is such that it is extremely unlikely that the Protocol will be terminated in its entirety. Should all parties unanimously wish to terminate the Protocol, a process to identify the future ownership of and confirm as necessary mutual rights to use any Shared Personal Data will be undertaken and completed prior to termination of the Protocol.

19 Where any of the parties ceases to be a separate legal entity, it shall:

(a) inform each and every SPoC in writing as soon as possible in order to draft and agree one or more written procedures for the deletion and/or return of any Shared Personal Data as necessary;
(b) be removed from the Protocol.

20 Any additional legal entity that wishes to be part of this data sharing Protocol may submit a request in writing to the University's Data Protection Officer. The consent of each and every party is required in order for the additional party to be included into this Protocol together with completion of contractual adherence to this Protocol.

21 In the event that a party is removed from the Protocol or a new legal entity joins the Protocol in accordance with clauses 19 and 20, an amended and updated version of this Protocol will be drafted as soon as practicable and circulated to all other parties.

22 The parties shall review the effectiveness of this data sharing Protocol every five years, or upon the addition and removal of a party, or upon the request of one or more of the parties, having consideration to the aims and purposes set out in clause 5, and to current Data Protection Legislation, and to any concerns raised at that time by one or more of the parties. The parties shall continue or amend the Protocol depending on the outcome of the review but in the meantime the Protocol shall continue in full force and effect.

23 Each party is responsible for their own legal compliance and self-audit. A party, however, reasonably may ask to inspect another party or parties' arrangements for the processing of Shared Personal Data and may request a review of the Protocol where it considers that another party is not processing the Shared Personal Data in accordance with this Protocol, and the matter has demonstrably not been resolved through discussions between the relevant SPoCs.

CHANGES TO APPLICABLE DATA PROTECTION LEGISLATION

24 Should the applicable Data Protection Legislation change in a way that the Protocol is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that the SPoCs will negotiate in good faith to review the Protocol in light of the new legislation but in the meantime the Protocol shall continue in full force and effect.

RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE DATA PROTECTION AUTHORITY

25 In the event of a dispute or claim brought by a Data Subject or a Data Protection Authority concerning the processing of Shared Personal Data against any or all parties, the parties will inform each other as necessary about the dispute or claim, and will cooperate with a view to settling the dispute or claim amicably in a timely fashion.

Signed by [NAME]	.....
for and on behalf of The University	[Title]
Signed by [NAME]	.....
for and on behalf of CAm	Director
Signed by [NAME]	.....
for and on behalf of the Colleges	Chair of Colleges' Committee

Schedule 1 Data protection principles and standards

LAWFUL AND FAIR PROCESSING

1.1 Each party shall commit to processing any Shared Personal Data lawfully, fairly and in a transparent manner and in accordance with the data protection principles in Article 5 of the GDPR.

1.2 Each party shall ensure that it processes Shared Personal Data under one or more of the legal bases in Article 6 of the GDPR and Data Protection Legislation.

1.3 In addition to its obligations under paragraph 1.2 of this Schedule 1, each party shall ensure that it processes Shared Personal Data classified as Special Category (Sensitive) Personal Data under one or more of the legal bases in Article 9 of the GDPR and applicable Data Protection Legislation.

1.4 Each party shall, in respect of Shared Personal Data, ensure that their data protection statements (or privacy notices) are clear and that they provide sufficient information to the Data Subjects in accordance with applicable Data Protection Legislation for them to understand what Personal Data is being shared with the other parties, the purposes of the data sharing, a contact point for the Data Subjects, and any other information to ensure that the Data Subjects understand how their Shared Personal Data will be processed. Each party shall retain or process the Shared Personal Data in accordance with the relevant data protection statement(s).

DATA SUBJECTS' RIGHTS

1.5 Data Subjects have the right to obtain certain information about the processing of their Personal Data (including Shared Personal Data) through a Subject Access Request. In certain circumstances, as defined in the GDPR, Data Subjects may also request rectification, erasure or blocking of their personal data and may exercise other rights.

1.6 SPoCs should endeavour to maintain a record of individual requests from Data Subjects, including the decisions made and actions taken.

1.7 The parties agree to provide reasonable assistance as is necessary to each other to enable them to comply with Subject Access Requests and to respond to any other rights requests, queries or complaints from Data Subjects.

DATA RETENTION AND DELETION

1.8 No party shall retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes. Parties shall continue, however, to retain Shared Personal Data in accordance with any statutory retention periods applicable in their respective countries and/or states.

DATA TRANSFERS OUTSIDE THE EEA

1.9 For the purposes of paragraphs 1.10 and 1.11 of this Schedule 1, transfers of Personal Data shall mean any sharing of Personal Data outside the European Economic Area (EEA), and shall include, but is not limited to, the following:

(a) storing Shared Personal Data on servers outside the EEA.
(b) sub-contracting the processing of Shared Personal Data to data processors located outside the EEA.
(c) granting third parties located outside the EEA access rights to the Shared Personal Data.

1.10 The parties shall only disclose or transfer the Shared Personal Data to a third party located outside the EEA in line with the provisions of Chapter V of the GDPR as implemented in the applicable Data Protection Legislation.

1.11 Transfers between CAm and the other parties will be made on the basis of the latest versions of the controller-to-controller or controller-to-processor EC-approved "standard contractual clauses" as published in the Official Journal of the European Union and which themselves form part of this Protocol.

SECURITY AND TRAINING

1.12 Each party shall only provide and receive the Shared Personal Data using secure methods, having regard to the availability of joint or shared IT systems, the technology for facilitate data transfers, the risk of data loss or breach and the cost of implementing such measures.

1.13 It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with any agreed technical and organisational measures to keep it secure and to uphold the data protection principles in Article 5 of the GDPR.