GCRB Glasgow Colleges' Regional Board

Performance and Resources Committee Meeting

Date of Meeting	Wednesday 7 March 2018
Paper Title	Shared Data Protection Officer
Agenda Item	12
Paper Number	PRC4-N
Responsible Officer	Jim Godfrey, Finance and Resources Director
Recommended Status	Disclosable
Action	For Noting

1. Report Purpose

1.1. To update the Committee on the recent developments in respect of a shared Data Protection Officer for the Glasgow region.

2. Recommendations

2.1. The Committee is asked to **note** that the three colleges and GCRB have agreed to collaborate on the appointment of a shared Data Protection Officer.

3. Background

3.1. The following text is reproduced from a paper produced by UCSS[1]:

- "The upcoming changes to Data Protection regulations (GDPR and, shortly, the UK-specific Data Protection Bill) take effect as of the 25th of May 2018 and will require a change to the way that the majority of our institutions operate in terms of the requirement to have a Data Protection Officer, and the duties they must perform. There are a number of implications and challenges to this, and a Shared Service offering has been requested by a number of our institutions to mitigate and manage this.

- The GDPR regulations…allow…a Shared Service Approach. It seems exceedingly likely that many organisations will be looking to hire DPO calibre candidates in the coming year.

- The duties of the Data Protection officer are defined by the regulation…but in summary - the DPO must not have operational responsibilities that would be a conflict of interest, and must report to the highest management level of the institution.

[1] UCSS (Universities and Colleges Shared Services) is a not-for-profit Shared Service organisation jointly owned by all Universities and Colleges in Scotland. It provides shared services to institutions and where applicable to sector owned bodies. Further information is available via the following link; http://www.ucss.ac.uk/#&home

- The consequence of this is that current organisation, and practice, of many of our institutions…will have to change in organisational terms, as well as ensuring that monitoring and advising on the more onerous regulations around Data Protection is performed.

- After engaging with the various stakeholders at many of our institutions…it is anticipated that…the majority of our institutions will not require a full time dedicated DPO…Many of our institutions are keen to budget/plan for a service or individual who can perform the DPO role as required by the GDPR legislation."

4. Collaborative Approach

4.1. The proposed way forward has been considered in detail at a national and regional level. As a result, the three Glasgow colleges and GCRB have agreed to pursue a collaborative model in respect of a shared Data Protection Officer with UCSS. It has been agreed that UCSS will appoint a (full-time) Data Protection Officer who will work on behalf of all four organisations. A copy of the job description for this post is attached as an annex to this document. Interviews for this post are taking place in mid-March 2018 and it is anticipated that an appointment will be made shortly thereafter.

4.2. The allocation of time, between each of the four organisations, has been agreed. The relative share has been determined by reference to the size of the organisation and also the existing staff currently employed by the college. The allocation of the average number of days per week of the Data Protection Officer will be as follows:

City of Glasgow College	2.00
Glasgow Clyde College	2.25
Glasgow Kelvin College	0.25
GCRB	0.25
Total	**4.75**

4.3. A copy of the (draft) Shared Service Agreement is attached for information.

4.4. This collaborative model is consistent with the Glasgow Region Strategic Plan for College Education and brings a number of advantages and benefits. For example, it:

- Enables all parties to address the risks posed by the new regulations.

- Allows all parties to gain access to an area of specialist expertise that will complement the current arrangements.

- Combines resources facilitating the four organisations to recruit one full-time Data Protection Officer.

- Allows all parties to support each other. For example, to provide cover between regions in the event of an absence, or urgent priority.

- Supports the sharing of expertise at a regional and national level (including access to a national Head of Data Protection Services).

5. Risk Analysis

5.1. The approach outlined above enables GCRB, and the Glasgow Region, to address the risks posed by the new regulations in respect of Data Protection and GDPR.

6. Legal Implications

6.1. There are specific legal implications associated with the implementation of General Data Protection Regulations (GDPR) in May 2018.

7. Resource Implications

7.1. The estimated cost of the shared Data Protection Officer is £57,000. The proportion of this cost that directly relates to GCRB is expected to be in the region of £3,000.

8. Strategic Plan Implications

8.1. There is a clear link between the regional strategic ambition of good governance and full compliance with relevant legislation. This report outlines a collaborative approach to the issue of Data Protection and GDPR.

UCSS POSITION PROFILE

JOB TITLE	**Data Protection Officer**
LOCATION	**Variable across relevant regions**
TENURE	**Permanent**
REPORTS TO	**Data Protection Officer – Head of Service**

Post Holder Name	
Post Holder Name should only be completed when this document is being used as a Development Matrix	

Purpose of the job

- The post holder will be the defined Data Protection Officer at each of their defined institutions within their regional portfolio, with a reporting line at each one, as required under the forthcoming GDPR, to an appropriate member of the senior management team.

- The roles will have multiple bases within a defined region and the DPOs will be expected to work locally at each of the institutions within their portfolio proportionally based on their size and business risk, as well as provide cross region cover for absence and incident management.

- The post holder must have a detailed knowledge of privacy related legislation and GDPR and will also have strong gravitas with outstanding communication skills, will be analytical with the ability to pay strong attention to detail.

- The post holder must be able to operate and gain respect of staff at all levels within institutions as well as where applicable, with students and other stakeholders.

- The post holder will operate data protection / information governance frameworks with particular focus on developing and performing oversight on the data protection risk and control environment, including the impacts to it from supply chain and internal processing and change activity.

- Be responsible for the analysis and reporting of the data protection risk and control environments ensuring timely identification of themes and emerging issues and making recommendation for action to allow reporting to relevant management and relevant Committees.

- Be responsible for developing and maintaining Data Protection Policies, ensuring they are kept up to date and in line with the organisations risk appetite and regulatory expectations.

- Deliver internal "consultancy" on data protection risk to institutional colleagues and support managers in managing data protection risks within their areas & promote and facilitate data protection risk awareness and understanding across client institutions through generic and targeted training.

Principal Responsibilities

				Development Matrix Use		
				Name:		
Name:		Name		Date:		
	Responsibility	Competency	Expected Level (see below)	Current Responsibility Yes/No	Current Level (if Current Responsibility)	Development Actions
1	Lead in delivering the statutory and contractual obligations of the DPO role within their client institution portfolio. (scope of specific service deliverables that can be expected by institutions of the DPO role as set out in the shared service agreements are summarised in Annex 1)	Leadership / Results Focus	3			
2	Deal with (including advising others to deal with) queries from business areas in respect of whether their current / planned activities are / will be GDPR compliant and helping to identify solutions.	Legal & Business Process	2/3			
3	Ensure ongoing compliance with GDPR and associated data protection legislation and work to raise privacy awareness within the institutions generally.	Legal & Business Process / Results Focus	2			
4	Be responsible for managing and implementing the framework of policy and procedures in the area of data protection, drafting policy, procedure and jointly developing privacy notices with business managers where required and ensuring that all required policies are in place and updated as required	Organisational Awareness / Legal & Business Process	3			
5	Work closely with the business, in particular in the areas of Marketing, Records Management, Information Security, Operations	Relationship Management / Legal &	2			

	and HR in ensuring data protection compliance within the institution.	Business Process				
6	Keep up to date with guidance and legislative change and be responsible for privacy training and awareness within the institutions	Legal & Business Process / Results Focus	2/3			
7	Deal with Data Subject Access Requests, Right to be Forgotten etc and other rights exercised by data subjects balanced against legal needs of confidentiality and of business need to retain data. competing	Legal & Business Process / Results Focus	2			
8	Where required, be the designated point of contact for data subjects and the ICO in connection with privacy related matters.	Legal & Business Process	2			
9	Advise the institutions on handling of any privacy breaches, working to identify root causes, mitigate risks and prevent reoccurrence. Support /advise the institution's management in dealing with data protection related complaints or investigations by the ICO.	Leadership / Legal & Business Process	2/3			
10	Approval of proposed data sharing arrangements and analysis of whether the sharing is to be on a controller/controller basis or a controller/processor basis. Consideration of proposed data exports and ensuring the requirements for the export are met. Provision of advise on local contract owners assessment of vendors data protection assurance information	Relationship Management / Legal & Business Process	3			
11	Assist / guide institutional management / staff in undertaking Privacy Impact Assessments where necessary including in connection with	Relationship Management / Legal & Business Process	3			

	significant change management projects.					
12	Develop tools and templates in relation to data protection management for use both in own institutions and across all DPO-Share members.	Legal & Business Process / Results Focus	2			
13	Provide ad hoc and periodic training for institutional staff	Organisational Awareness / Legal & Business Process	2			
14	Provide sound commercial advice to senior management teams / Boards on relevant privacy risks.	Organisational Awareness / Legal & Business Process	3			
15	Prioritise team projects in line with the needs of the business and risk levels.	Leadership	2/3			

Knowledge and Skills

- Be of intellectual calibre, with the highest ethical standards;
- Be a professional, credible manager with excellent general management skills and have the essential competencies of clarity of purpose, self-confident integrity and strong influencing power; and
- Have good knowledge in the development, implementation and maintenance of IS solutions and in particular of how they are applied and utilised in the HE/FE sectors
- Strong experience of managing and working with data protection / information governance frameworks with particular focus on developing and performing oversight on the data protection risk and control environment, including the impacts to it from major change activity
- Track record in delivering practical and compliant data protection controls / solutions
- Experience in information governance, business risk management, audit or information security
- Ability to challenge colleagues in a collaborative and constructive manner to drive a pragmatic risk approach to data protection risk mitigation
- Excellent negotiation, influencing, relationship management and communication skills and able to translate complex / technical issues to meet the audience's competency level and in their 'language'
- Passion and enthusiasm to follow developments in privacy and data protection, and maintain a professional expertise and personal interest in these subjects
- Have an excellent knowledge (or clearly demonstrate the ability to obtain) of the HE/FE sector stakeholder landscape
- Have skills in meeting demanding targets and deadlines on a day to day basis
- Strong planning and organisational skills

Experience

- Good experience of working within teams and the ability to build relationships at all levels
- Understanding of public sector governance arrangements
- Have experience in implementation / development of business systems
- Comprehensive data management information experience
- Significant reporting / analytical experience. Advanced spreadsheet skills and the ability to use financial models to present efficiency performance

Contacts and Relationships

- They will possess the personal qualities to work with personnel across the HE/FE sectors as a persuasive ambassador for their area of expertise. They will build effective and collaborative relationships and will achieve support and buy in from gaining respect that than simply relaying of the definition of the role.
- Excellent verbal and written communication and interpersonal skills
- Good problem solving and influencing skills in dealing with a diverse range of stakeholders

Competencies relevant to this role

Level 4 is strategic business leader level competency, level 3 is senior level, 2 is advanced level, 1 is operational level. Note that some competencies are at their highest requiring a level of competency below 4, but a lower number can still therefore require total / complete ability in delivering in this area.

LEADERSHIP	
DEFINITION : Contributes to the achievement of team goals by providing support, encouragement and clear direction when appropriate.	
Attribute	
Leads and supports team	Clearly delivers / commands high levels of leadership and support. Will adopt principles confidently and will encourage institutional staff to undertake their roles effectively in relation to data protection management.
Delegates duties and responsibilities	High level of understanding and effectively plans and delivers delegation activities. Will understand where to establish balance between undertaking activities personally as opposed to advising institutional staff / stakeholders where they will need to deliver data protection related activities in line with business priorities.
Coaches and mentors staff	Clear understanding of the concept and will support, encourage and develop others in a dynamic way.
Leads and directs meetings	Understands clearly. Will lead and direct meetings (internal, cross functional, or with external organisations such as supplier's) in order to achieve business objectives.
Decision making	Can resolve more complex issues that cross a number of work groups. Consults with stakeholders and always makes sound judgements that may influence policy. Applies analytical techniques in decision making process.

LEGAL and BUSINESS PROCESS CAPABILITY	
DEFINITION : Has the knowledge and understanding of relevant legal and DPO business process management	
Attribute	
Legal Knowledge	Maintains comprehensive expert level legal knowledge of all matters that relate to data protection management, including data legislation, contract (staff and business) and statutory data management / retention law, FoI legislation etc.
Data protection	Provides expert level advise and management skills in all matters related to both personal and business data protection.
Data Management and Control	Leads / advocates the use of appropriate data management and control systems. Is sought after for advice both in current data use, and future data / reporting process and system development. Applies similar techniques to own "uncontrolled" data and information.
Initiates and manages change	Develops the change message and communicates the impact and nature of change. Encourages others to participate in the process of change. Provides clear plans for change, pushes for and ensures implementation
Key Sector Systems & tools (e.g. ERP/Fi, Student Records, VLEs, hardware equipment and infrastructure etc)	Comprehensively understands key sector systems and tools, and how data is used in / around them.
Manages risks	Leads the development of risk analyses, assessments and management plans for complex projects. Conversant in the terminology of risk and provides guidance to other staff.
Sourcing and Tendering Support	Understands that sourcing and tendering are an essential and value adding part of a fuller strategic management process. Responsible for advising stakeholders on data protection matters in relation to external organisations – assessment at tender / selection stage and for monitoring ongoing compliance.
Specification Development	Develops appropriate data protection specifications with / for customers

ORGANISATIONAL AWARENESS	
DEFINITION : Clearly understands roles and responsibilities, how Information Governance should be organised, the value it can bring and where it should sit within organisations	
Attribute	
Identifies roles and responsibilities	Clearly understands different roles and responsibilities, not just within own role, but within other business functions and organisations. Is able to direct information based on knowledge.
Positions DPO within organisation	Clearly understands where Data Protection sits within own sector structure and the wider public sector. Can eloquently articulate views and influence on where the Data Protection role should position itself.
Can identify various organisational structures	Clearly understands when a structure needs changing and can propose alternative structures for consideration.
Implements policy	Experienced in policy development. Leads / advises on policy changes and development as applicable. Has specific knowledge of key aspects of policy, and provides guidance to others.
Recognises wider objectives	Highly knowledgeable in how external decisions impact the organisation. Will modify process, policy and practice to adapt to such changes.
Takes cognisance of Political, Economic, Social & Technical (PEST) factors affecting the DPO function.	Good understanding of the implications and how these factors may impact on the business or DPO function. Will plan, and take appropriate action to address relevant issues.
Training	Can deliver clearly and confidently. Aware of the audience, their understanding and differing needs

RELATIONSHIP MANAGEMENT	
DEFINITION : Identifies different types of customers and stakeholders and formulates strategy for managing relationships	
Attribute	
Manages customer relations	Very knowledgeable of customer issues. Can handle complex customer issues, providing a real sense of ownership. Owns the issue to resolution and provides support to other staff.
Differentiates between internal & external customers needs	Is able to interpret customer needs. Will pre-empt customer issues based on assessment of customer type.
Flexes strategy according to customer focus	Knows when to change customer strategy and flexes strategy according to customer priorities.
Recognises wider implications of actions	Knowledgeable of internal and external implications of decisions. Will modify process, policy and practice to adapt to such changes. Will be sought after for advice.
Markets Data Protection	Good understanding of the process and the concept of marketing Data Protection. Is aware of the impact on internal and external stakeholders.
Engages with key stakeholders	Has an in-depth knowledge of key stakeholders. Skilfully manages their expectations through the application of identifiable stakeholder management techniques such as stakeholder maps.
Influencing internal and external customers / stakeholders	Has in-depth knowledge of how to use influencing skills. Will use these to lead others to a decision or action.
Establishes collaborative partnerships (e.g. Cross functional / organisational) teams, cross sector collaborative working, or commercial partnering arrangements.	High level understanding of collaborative approaches. Able to follow but also create effective procedures. Understands issues and benefits of collaboration. Sufficiently knowledgeable to recognise when to seek advice and other support.

RESULTS FOCUS	
DEFINITION : Is aware of how personal and team objectives contribute to the success of the organisation and continually demonstrates commitment to achieving these.	
Attribute	
Sets key performance indicators	Has expert understanding. Can identify when corrective action is necessary and able to identify the appropriate action to be taken in relation to individual and departmental KPIs/BPIs. Is able to demonstrate originality in the development of KPIs/BPI's in response to business requirements.
Monitors quality and plans to meet timescales for delivery	Demonstrates ongoing commitment to achievement of personal and institution goals within timescales and budgets. Will recommend corrective action.
Agrees objectives in line with wider organisational needs	Demonstrates very clear understanding of how DPO objectives are linked to an overall organisational / sectoral plan.
Measures performance against objectives	Will have leading role in measuring results against objectives. Anticipates factors that affect performance and takes corrective action.
Reports performance to key stakeholders	Clearly understands the purpose of performance reporting. Will stress need to achieve and will prepare reports to key stakeholders.

Annex 1

The following services will be offered to be delivered by the Shared Services Resources (SSRs), i.e. the Data Protection Officers (DPOs):

- Act as DPO in fulfilling the statutory obligations of the role wherever empowered to do so.
- Provide experience, expertise and legal guidance in Data Protection and GDPR
- To review and update periodically each institution's data protection policy and supporting procedures
- To have knowledge of case law / ICO decisions and disseminate learnings as applicable to relevant stakeholders / staff – to recommend actions and issue guidance informed by this
- To provide annual data protection assessments, compliance audits & compliance reports to governing bodies / senior management teams as required.
- To achieve a fundamental understanding of the sector to ensure pragmatic, proportionate and workable guidance and support is delivered, using balanced judgement
- Participation in operational meetings and offering advice on how regulations impact upon the institution
- Provide / offer training to institutional staff
- Approach service delivery in a tailored way taking account of each institution's different environment / circumstances. Contextualise guidance in different functional areas within institutions (HR, Finance etc.). But while ensuring advice is consistent with that provided to other shared service members
- Develop and support use of data protection assessments tools and templates (privacy assessment tools etc) and share them across *DPO-Share* SSRs / utilise tools templates as developed by other *DPO-Share* SSRs within the institution to maximise efficiency
- Undertake breach investigations and report matters to senior management. Note that the SSR will not report breaches to the ICO unless specifically requested to do so (the reporting or not of breaches to the ICO is a decision for institutional management to make).
- The SSRs would be available over the phone / email for urgent questions/advice even if at a work day at another institution. SSR where it is practical and appropriate may not always be on-site for a workday for a particular institution (although they normally will)
- Each member of *DPO-Share* commits to enable flexible utilisation of the services to suits particular needs of membership, this could include (depending on the breach / the work involved) diverting of a resource to cover a breach situation at another member / SSR region, the SSRs would ensure that the resources over time (normally within a month) are however consumed in line with FTE share levels
- The SSR will adhere to institutional confidentially as appropriate and not share relevant matters with other members.

Shared Services Agreement – DPO Shared Service ("*DPO-Share*")

Agreement Between the Parties:

The Glasgow Colleges' Regional Board an unincorporated body with Robert Ashton as the Accountable Officer
Glasgow Clyde College, 690 Mosspark Drive GLASGOW G52 3AY, SC021182,
Glasgow Kelvin College, 123 Flemington St, Glasgow G21 4TD, SC021207
City of Glasgow College, 190 Cathedral Street, G4 0RF, SC036198
("XCs")

And

APUC Ltd, Stirling Business Centre, Wellgreen, Stirling, company number SC314764 ("UCSS")

Where

Glasgow's Colleges, which this agreement is agreed to primarily serve, are members / part owners of UCSS (with Glasgow Colleges' Regional Board (GCRB) an Associated Body), which is company limited by guarantee owned / guaranteed by its member institutions.

This "Agreement" is not a commercial / purchasing based agreement, it is a risk sharing shared service agreement provided for under the Teckal exemption. It is intentionally not written as a legalistic document to cover every eventuality, it aims to set out ways of working and to provide clarity over what each Party is committing to on the basis of it being a shared service between trusted partners.

This Agreement is for use of named Data Protection Officers (DPO) as part of a sector shared team to meet institutions' statutory requirements based on the General Data Protection Regulation (GDPR), to have an effective, named DPO in place. This agreement is to provide named DPOs for Glasgow Clyde College, Glasgow Kelvin College and GCRB, with a much more limited advisory service provided to the City of Glasgow College.

Commencement Date

The services and the relevant charges that this Agreement shall cover shall commence as soon as relevant resources are in place (recruitment under way) – estimated to be during March /April 2018.

Background

UCSS's core purpose is to operate as a centre of procurement expertise across the Scottish HE/FE sector in line with the requirements of the Public Procurement Reform Programme. For this core purpose, UCSS receives collective sectoral funding.

Further to this however, several institutions, have requested that UCSS provide other resources focussed at institutional level on a shared service model.

XCs have recently undertaken a review of their operations in relation to having DPO services in meeting the statutory needs of the GDPR and have identified that they wish to obtain this service as part of the UCSS *DPO-Share* arrangement.

UCSS and XCs have agreed that the following will be provided by UCSS on a shared service model:

Operational Arrangements & Scope of Service

FTE	Level of Resource Required
GCRB 0.053 FTE (0.25 days per week)	Data Protection Officer
Glasgow City (Associate Member) 0.053 FTE (0.25 days per week)	DPO Advisory Service
Glasgow Clyde College 0.473 FTE (2.25 long days per week)	Data Protection Officer
Glasgow Kelvin College 0.421 FTE (2 long days per week)	Data Protection Office

The following services will be offered to be delivered by the SSRs:

- Act as DPO in fulfilling the statutory obligations of the role wherever empowered to do so.
- Provide experience, expertise and legal guidance in Data Protection and GDPR
- To review and update periodically each institution's data protection policy and supporting procedures
- To have knowledge of case law / ICO decisions and disseminate learnings as applicable to relevant stakeholders / staff – to recommend actions and issue guidance informed by this
- To provide annual data protection assessments, compliance audits & compliance reports to governing bodies / senior management teams as required.
- To achieve a fundamental understanding of the sector to ensure pragmatic, proportionate and workable guidance and support is delivered, using balanced judgement
- Participation in operational meetings and offering advice on how regulations impact upon the institution
- Provide / offer training to institutional staff
- Approach service delivery in a tailored way taking account of each institution's different environment / circumstances. Contextualise guidance in different functional areas within institutions (HR, Finance etc.). But while ensuring advice is consistent with that provided to other shared service members

- Develop and support use of data protection assessments tools and templates (privacy assessment tools etc) and share them across *DPO-Share* SSRs / utilise tools templates as developed by other *DPO-Share* SSRs within the institution to maximise efficiency
- Undertake breach investigations and report matters to senior management. Note that the SSR will not report breaches to the ICO unless specifically requested to do so (the reporting or not of breaches to the ICO is a decision for institutional management to make).
- The SSRs would be available over the phone / email for urgent questions/advice even if at a work day at another institution. SSR where it is practical and appropriate may not always be on-site for a workday for a particular institution (although they normally will)
- Each member of *DPO-Share* commits to enable flexible utilisation of the services to suits particular needs of membership, this could include (depending on the breach / the work involved) diverting of a resource to cover a breach situation at another member / SSR region, the SSRs would ensure that the resources over time (normally within a month) are however consumed in line with FTE share levels
- The SSR will adhere to institutional confidentially as appropriate and not share relevant matters with other members.

This delivery model is based on estimated requirement to comply with new and untested legislation, it is likely that there will be significant and sometimes competing demands on their time. The SSRs therefore will prioritise their time within an institution's allocation based on business priorities, compliance needs and risk.

UCSS would assess the relevant skill and competency levels. As this is a newly regulated profession, UCSS will, with the guidance of the Steering Group, establish the most effective way to obtain the relevant resources which may, until the roles are more widely established and available on the market, include targeted GDPR training for staff with appropriate information management / governance backgrounds to deliver the service.

This role would locally report to the following within XCs:

GCRB: xxxxxxxxxxxx
Glasgow Clyde College: xxxxxxx
Glasgow Kelvin College: xxxxxxx
City of Glasgow College: xxxxxx
[legally needs to be whoever heads up governance or the Principal in the case of institution taking the full DPO Service]

The shared service resources will operate as if they were a member of institutional governance staff.

Limitations

The shared service resources (SSR) will be responsible for delivery of statutory shared services within the institution as set out in the General Data Protection Regulation (or a subset of these if that is specifically agreed).

UCSS SSRs do not have executive / mandatory authority over institutions or staff within them that it provides the shared services to. The subject matter is also in an unclear emerging / developing environment so services by the very nature of them can only be provided on a best endeavours basis. UCSS therefore cannot accept any liability for any impacts related to utilisation of services in relation to this Agreement and the DPO-Share service.

Governance of Service / Annual Review

A Steering Group will exist with one place reserved for each member institution using the shared services. The Steering Group will provide direction on how the resources are used, what future charging models may be appropriate and to provide direction on future development of the shared service. Attendance at Steering Groups will not be mandatory but if an institution's representative person does not attend (either physically or by video / tele conference), unless they appoint a proxy, it is assumed that they are in support of any majority decision made.

As this service is new and for a new business need, a review shall take after 12 months and any changes to take account of experience to date as agreed by the Steering Group, will be put in place as soon as possible thereafter.

Staffing & Employment Costs

UCSS is delivering this as a shared service at the request of XC and other members at estimated averaged actual cost and not as a commercial venture.

The *DPO-Share* service will be managed as a separate cost centre and resource pool within UCSS. Employment costs incurred therefore will be charged at actual costs to the users of the service. In the event of loss of resource through sickness, jury duty, parental leave etc, service impacts, the staff costs due will still be charged to relevant institutions. Days lost in this way will be spread proportionately across all institutions that the particular DPO serves. Obviously however UCSS would manage resources to minimise non-productive time and ensure the work is delivered as efficiently and effectively as possible.

Although each institution will have a named DPO, UCSS reserves the right to substitute staff provided to fulfil this Agreement (UCSS will however provide its best endeavours to ensure that inappropriately frequent substitution is avoided), and in providing emergency cover from elsewhere in the team, for example if an institution has a data breach when their named DPO is on leave.

In order to ensure that the SSRs are kept up to date with topical professional, developmental and legal issues effecting their jobs, the staff will be required to take part in joint team events ("Open Forum days") every 2-3 months. These, along with holidays / absence etc would be spread proportionately across each of a DPOs regional clients (managing this aspect across the whole country would be too complex to manage). The staff covered by this Agreement would of course, technology permitting, remain connected to the XC communication network to deal with any critical issues.

TUPE

It is not intended that any existing staff within an institution would have rights under TUPE. If in relation to this Agreement, TUPE is found at any time to be relevant however, all Parties would comply with legislation if / as applicable at the time.

Cost Distribution / Financials

The structural model for this service is to employ one coordinating / managing DPO to manage the team and have regionally based DPOs elsewhere (servicing institutions within a reasonable distance of their base). They would be based for HMRC expenses purposes in the location closest to where most of their time would be consumed (to minimise claimable expenses). It would not appear fair for one region to pay a higher overall cost due to that particular region being the one where the coordinating DPO is based so all costs for all DPOs would be added together and then split equally across the members of the shared service proportionately based on their level of FTE service committed (they would be line managing and coordinating delivery across all regions).

Costs are separated into three different types:

- "Resource Costs" – this includes salaries, pension contributions, NI and general overheads (this includes training / development / conference attendance (including travel accommodation to training / conferences and to UCSS corporate events – Open Forum days etc) and normal employment overheads). Travel costs for the Managing DPO to meet / line manage SSRs in other regions are also included within Resource Costs. Resource costs are, as noted above, calculated by combining the total Scotland wide cost of all *DPO-Share* staffing to achieve an average FTE SSR resource cost which is charged at the same rate to all members. These costs will be charged to members quarterly in advance.

- "Variable Costs" – this includes travel expenses for travel of SSRs beyond their base location to other members within the region (if more than 10 miles from their base location) and other travel reasonably required for them to do their job (except for the areas specifically covered in Resource Costs above). These costs will be charged to members quarterly in arears based on actual claims submitted in line with UCSS's travel policy etc. The costs will be combined into one sum for each SSR's region / customer portfolio then charged based on the FTE split to each member within that region / portfolio (in order not to disadvantage institutions where the SSR does not happen to be based at) – not Scotland wide.

- "Tailored Costs" – these are costs that may be incurred by specific request(s) from individual institutions – for example if one institution requires a SSR to be Disclosure Scotland checked or travel abroad for business. These are charged only to the institution(s) that have requested the specific cost to be incurred, normally charged in arears.

The maximum estimated Resource Costs of provision of this shared service are stated below, these costs will only be varied upon changes to costs of providing the service and any changes shall be required to be agreed by the Parties in writing (except as set out below). This shall not normally be more frequent than annually and will be aligned to academic years. The costs may be below the maximum level stated below and if so they will invoiced at that lower level - they will be charged

based on the average shared costs for DPOs – this may vary as staff leave and be recruited from time to time.

Any pay adjustments based on an UCSS's cost of living pay award (applicable to all UCSS staff) will automatically be deemed to be acceptable to XC and not require specific approval but any changes beyond this will be required to be approved by XC.
The costs applicable are set out below (for 2017/18 year – 2018/19 will be plus basic UCSS cost of living increase agreed by the UCSS Board at the time).

Role	Resource (FTE) Costs (excl travel) FTE = 4.75 long days / week	FTE level	Maximum Annualised Resource Cost based on FTE split	Monthly Cost
Data Protection Officer for GCCB	*0.25 long days per week*	*0.053*	*£3,042.20*	*£253.52*
Data Protection Officer for Glasgow Clyde College	*2.25 long days per week*	*0.473*	*£27,150.20*	*£2,262.52*
Data Protection Officer for Glasgow Kelvin College	*2 long days per week*	*0.421*	*£24,165.40*	*£2,013.78*
DPO Advisory Service for City of Glasgow College	*0.25 long days per week*	*0.053*	*£3,042.80*	*£253.52*

If demand for the service requires further similar staffing provision, the parties may agree for this provision by separate emails (including at what level such staffing should be employed at) but will be in accordance with the terms and conditions set out in this Agreement and shall then be deemed to be part of this Agreement.

Payment terms shall be 30 days from date of invoice.

The above is based on a minimum 35.5 hour working week *(expected to be worked over a 9.5 day fortnight).* The staff member would be salaried so no overtime payments would apply.

All cost mentioned are excluding VAT. As this charging model is based on "shared reimbursement" rather than "exact reimbursement", VAT may need to be charged on these services (in dialogue with VAT advisers / HMRC at present).

Workspace Accommodation

Clients will provide and fund suitable desk-space and relevant work equipment etc for the SSRs while they are working on their campuses. Laptops and Smart phones will be provided by and funded by UCSS from the standard fees paid.

Confidentiality and Data Security

UCSS shall take all reasonable steps to keep information handled under this Agreement secure and safe.

Any information supplied by one Party to another Party in connection with this Agreement shall remain the property of the original owner and any information derived from or otherwise communicated to a Party in connection with the Agreement shall be kept secret and shall not, without the consent in writing of the owner of the information, be published or disclosed to any third party, or be made use of by the any Party except for the purpose of delivering the shared services.

The Parties accept however that even if information is held to be confidential, that a Party may be required under law or regulations or in order to perform their work, to disclose such information to other parties. Disclosure under these scenarios shall not be considered a breach of this section therefore.

.

The Parties and any third parties (including individual consultants) appointed through them who are involved in delivering the services / related services are contractually obliged (the relevant hiring Party shall ensure this is applied) to operate within the requirements set out in this Agreement and under relevant data protection legislation.

In the event that UCSS acquires any Personal Data (as defined in the Data Protection Act / GDPR), UCSS shall keep such information confidential and shall only process such data in accordance with the relevant regulations and law.

The provisions of this section shall apply during the continuance of this Contract and after its termination.

Intellectual Property Rights

“Intellectual Property Rights (IPR)” being intellectual property owned by a person or organisation or a right to use intellectual property.

Each party who provides IPR which is used in the delivery of the services shall retain ownership of it. It is agreed by the Parties that any tools, materials etc provided to UCSS by any Client that is for the purposes of providing DPO services, will be provided under the spirit of collaboration and UCSS and any other (client) Party is permitted to use these materials if provided via the DPO service without any charge beyond their normal contribution to shared service costs.

The Parties warrant that in respect of any IPR owned by any third parties and which is used in the provision or receipt of the services, including software used in supporting processes / services to the core service, that they have obtained all necessary permissions and licenses to use such IPR. Any Party that breaches this clause shall accept full responsibility for such breach and make good the situation without detriment to any other Party.

Any IPR created in the course of managing delivery of the shared service (including governance and guidance, materials, tools and any technical developments) is deemed to be owned by UCSS and shall be freely available for use by members of the DPO shared service but shall not be used by them for commercial gain.

No Party has any rights to use in any way, to any IPR owned by another Party that they may come across in the delivery of the shared service unless it is reasonably required to perform the service and related activities.

Core Contacts

The Core Contacts in each of the Parties is:

UCSS: Angus Warren

GCRB: xxxxxxxxxxxxxxx
Glasgow Clyde College: xxxxxxxxxxxx
Glasgow Kelvin College: xxxxxxxxx
City of Glasgow College: xxxxxxxxxxxxx

Termination

The minimum duration of this Agreement is until 31st July 2020, beyond this, any Client Party (or indeed UCSS if required by their Board) may terminate their utilisation and commitment to the service giving the other 6 months' notice in writing, delivered by email (if an acknowledgement of receipt is provided) or by recorded post (to clarify, to terminate end July 2020, notice would be required by January 2020).

Aside from this, if the shared service over time (including before the July 2020 date) becomes uneconomic for UCSS to provide due to insufficient income for example through reduced institutions taking part, the service would be terminated in an orderly manner in line with the relevant funding.

After 12 months full operation however, the DPO Steering Group will review resource utilisation and needs and if changes to resource modelling are agreed, then such changes to resource levels and resulting change to charges will be applied at the earlier opportunity.

On ending of this Agreement duration or in preparation for the ending of this Agreement or if adjustments are made based on the 12 month review, UCSS will aim to re-allocate the resources. If suitable alternative employment is not found however within a reasonable period and if no other options are available, then the staff covered by the Agreement would be made redundant based on APUC's standard redundancy policy. This redundancy cost would be funded from the DPO Shared Service cost centre budget.

Governance of Agreement

Force Majeure. Neither Party shall be liable for failure to perform its obligations under the Agreement if such failure results from circumstances which could not have been contemplated and which are beyond the Party's reasonable control. The obligations of the Parties under the Contract will be suspended until such circumstances have eased.

This Agreement document and any subsequent amendments to it agreed by the Parties shall take precedence over any other contract, agreement etc between the Parties already existing for the service.

The Parties do not intend that any terms of the Agreement shall be enforceable by virtue of any legislation by any person who is not a Party to the Agreement.

If any provision of this Agreement is found by any court, tribunal or other administrative body of competent jurisdiction to be unenforceable or unreasonable it shall, to the extent of such illegality, invalidity, voidability, unenforceability or unreasonableness, be deemed severable and the remainder of the provision shall continue in full force and effect.

The construction, validity and performance of the Agreement shall be governed by Scots law and be subject to the exclusive jurisdiction of the Scottish courts.

Agreed For the Parties:

For APUC Ltd (UCSS)	
Name	Angus Warren
Position	Chief Executive
Signature	

For GCRB	
Name	
Position	
Signature	

For Glasgow Clyde College	
Name	Angus Warren
Position	Chief Executive
Signature	

For Glasgow Kelvin College	
Name	
Position	
Signature	

For City of Glasgow College	
Name	
Position	
Signature	