Doc 1

General Data Protection Regulations: Changes to lawful data processing.

Proposed plan of action

In May 2018 the General Data Protection Regulations (GDPR) come into force in the UK, replacing the Data Protection Act 1998. In 2016 the ICO issued guidance around the 12 main changes. This paper details the proposed response to 10 of these areas.

Information Asset Register, Legal Processing and Consent

Four of the 12 areas can be addressed with a combined course of action:

1. **Information you hold** - You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.
2. **Communicating privacy information** - You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
3. **Legal basis for processing personal data** - You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.
4. **Consent** - You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

The ICO is in the process of issuing detailed guidance on each of the 12 areas and the Consent document was issues for consultation on the 2nd March 2017. To summarise the guidance:

- Consent means offering individuals genuine choice and control.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of consent by default.
- Keep your consent requests separate from other terms and conditions.
- Be specific, granular, clear and concise. Vague or blanket consent is not enough.
- Name any third parties who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Remember – you don't always need consent. If consent is too difficult, look at whether another lawful basis is more appropriate.

City relies heavily on consent in its marketing and *Alumni* services as well as in schools. Examples include:

- Sending out a postgraduate prospectus five years after graduation
- Inviting *Alumni* to networking events or guest lectures

In most cases a student gives City their personal data as they have entered into a contract with City to provide them with an education. City can then process their data by virtue of the second lawful basis:

The processing is necessary: in relation to a contract which the individual has entered into

Once the contract has ended (graduated or failed to finish) the lawful reason to process their data ends and a new basis must be found. In most cases this is consent. Without the individuals consent we cannot use their personal data including contact details. Under GDPR this consent will have to comply with the guidance issued by the ICO.

High level proposed plan of action:

- City will need to identify what personal data it holds, where it came from and who we share it with. The formation of an Information Asset Register (IAR) is one of the seven objectives of the Information Governance Working Group and will commence shortly.
- Once Information assets have been identified the data flows will need to be mapped, the legal basis for processing identified, any privacy notices reviewed and 3rd party sharing documented.
- If the legal basis for processing is consent it will need to be reviewed and updated to comply with the ICO guidance.
- All current students and alumni will need to be contacted to 'opt-in' to the GDPR compliant consents.
- The consents and privacy notices will need a mechanism to be recorded and stored. This will depend of where we find the need for consent and may be on a per system / information asset basis or in a centralised location.
- Processes for individuals to manage their consents will need to be developed.
- An awareness campaign should be launched to educate users of personal data the changes brought by GDPR.
- Business processes involving non-GDPR compliant processing will need to be amended to only use data with a lawful basis (such as schools no longer holding local *Alumni* databases).

Development projects

In addition to the steps above a further two main areas of change can be packaged up into discrete development projects for other members of IT staff to take on. These are:

1. **GDPR Awareness campaign** – Following suitable training, plan, design and execute an awareness publicity campaign. This is to be done in conjunction with Marketing. Skillsets developed include: Project Management, Data Protection, Marketing, Working with other departments and communications. This would be a 10 day project split over three months.
2. **Right to be forgotten** - For each of our core systems holding personal data perform business and technical analysis on how to delete a subjects personal data. Produce a process and procedure which can be followed should a subject request to 'be forgotten'.

Areas of minor change for City

There are four out of the 12 areas which will only require minor change to City as they are aimed at different sectors or have already been established:

1. **Children -** GDPR states; 'City will need to put systems in place to verify ages and get parental consent for any data collection on children. Parental consent for children under 18 is currently collected, but Information Compliance will be raising awareness of the specific requirements under GDPR for children as part of its general awareness and training and as part of the work to ensure our procedures for collecting consent are compliant with GDPR.
2. **International -** GDPR states; "If you organisation operates globally you should make sure what supervisory authority different parts of your organisation falls under" Information Compliance is reviewing monitoring and advising on City's third parties processing agreement- especially processors based outside the EU and with the ever changing landscape of "Safe harbour" and 'Privacy Shield" arrangements.
3. **Subject access requests -** GDPR states; 'City should think about how it will handle requests within the new timescales and provide any additional information. At present, City, complies with SARs within 40 calendar days, this will reduce to 30 calendar days. City is well placed to be complaint with this new time scale.
4. **Data breaches** - GDPR states; 'City should ensure it has the right procedures in place to detect and investigate a personal data breach'. Information Compliance have produced an Information Security Policy available on the staff hub and produced a data breach form to enable swift reporting and investigations of any suspected breach- available on Service Now

Outstanding areas of change

This leaves two of the 12 areas still to be addressed:

1. **Data protection by design and data protection impact** assessments - GDPR states; City should plan how it will pass a privacy impact assessment, and implement any changes required to be compliant'. Information Compliance have developed, produced and promote Privacy Impact Assessment Guidance. All core IT systems holding or processing personal data should have a PIA performed before May 2018. Work has started on this but progress is slow.
2. **Data protection officers** - GDPR states; City should have a designated data protection officer'. Although City has two suitably trained DPOs they do not report to the highest level of management. Work will need to be done to alter the role of the DPO and ensure correct reporting lines.

New interpretations of GDPR content are published daily and this plan is subject to change if there is a shift in current thinking.

[redacted]

Action Plan				**Development Projects**		**Minor changes**				**Still to be planned**	
Information City holds	Communicating Privacy Information	Legal basis for processing	Consent	GDPR Awareness	Right to be forgotten	Children	International	Subject Access Requests	Data Breaches	Privacy by design	Data Protection Officers
• City will need to identify what personal data it holds, where it came from and who we share it with. The formation of an Information Asset Register (IAR) is one of the seven objectives of the Information Governance Working Group and will commence shortly. • Once Information assets have been identified the data flows will need to be mapped, the legal basis for processing identified, any privacy notices reviewed and 3rd party sharing documented. • If the legal basis for processing is consent it will need to be reviewed and updated to comply with the ICO guidance. • All current students and alumni will need to be contacted to 'opt-in' to the GDPR compliant consents. • The consents and privacy notices will need a mechanism to be recorded and stored. This will depend of where we find the need for consent and may be on a per system / information asset basis or in a centralised location. • Processes for individuals to manage their consents will need to be developed. • An awareness campaign should be launched to educate users of personal data the changes brought by GDPR. • Business processes involving non-GDPR compliant processing will need to be amended to only use data with a lawful basis (such as schools no longer holding local *Alumni* databases).				**GDPR Awareness campaign –** Following suitable training, plan, design and execute an awareness publicity campaign. This is to be done in conjunction with Marketing. Skillsets developed include: Project Management, Data Protection, Marketing, Working with other departments and communications. This would be a 10 day project split over three months. **Right to be forgotten -** For each of our core systems holding personal data perform business and technical analysis on how to delete subject's personal data. Produce a process and procedure which can be followed should a subject request to 'be forgotten'.		**Children** - Parental consent for children under 18 is currently collected, but Information Compliance will be raising awareness of the specific requirements under GDPR for children as part of its general awareness and training and as part of the work to ensure our procedures for collecting consent are compliant with GDPR. **International** - Information Compliance is reviewing monitoring and advising on City's third parties processing agreement- especially processors based outside the EU and with the ever changing landscape of "Safe harbour" and 'Privacy Shield" arrangements. **Subject access requests** - At present, City, complies with SARs within 40 calendar days, this will reduce to 30 calendar days. City is well placed to be complaint with this new time scale. **Data breaches -** Information Compliance have produced an Information Security Policy available on the staff hub and produced a data breach form to enable swift reporting and investigations of any suspected breach- available on Service Now				**Data protection by design and data protection impact assessments -** All core IT systems holding or processing personal data should have a PIA performed before May 2018. Work has started on this but progress is slow. **Data protection officers -** Although City has two suitably trained DPOs they do not report to the highest level of management. Work will need to be done to alter the role of the DPO and ensure correct reporting lines.	

DOC 2

Executive Committee are asked to **note** this report on the progress of the working group.

Information Governance Working Group – Progress Update

In August 2015 the Executive Committee approved the formation of the Information Governance (I.G.) Working Group. This group had seven key objectives:

1. I.G. Sub-Committee reporting into Executive Committee (ExCo)
2. I.G. Role structure
3. I.G. Policy and framework
4. I.G. Staff training and awareness programme
5. University wide information discovery exercise and review
6. Information asset register and controls
7. I.G. audit method and schedule

During March and April 2017 Information asset owners (IAOs) have been identified and offered training. The take up has been brisk with the following numbers trained after three sessions:

School or Service	**Attendees**
CLS	1
Finance	3
Graduate School	1
IT	5
Research and Enterprise Office	4
SASS	7
SHS	2
SMCSE	1
Strategy and Planning	1
Student and Academic Services	2
DARO	1

Please note Library, Marketing, LEaD and PaF have not yet been approached in regards to Information Governance. Initial conversations will take place in May.

Considerable progress has been made and work has now started to identify and record information assets in the Information Asset Register (IAR). After being recorded the assets will undergo classification and risk assessment.

The General Data Protection Regulations (GDPR) become law in May 2018. As part of demonstrating compliance with the new regulations the University must be able to show what information we collect, process and retain. Populating an IAR is key to achieving this

As this work is being performed two final work streams will begin:

Staff training and awareness: An awareness campaign will be planned and executed. This had been delayed as training the initial IAOs Initial conversations have been held with Marketing This will include the launch of a recently procured online e-learning module. The need for all staff to undertake Information Governance and Data Protection training was recognised by the Executive Committee in 2016.

The Information Governance Sub-Committee: The Information Governance Working Group will be disbanded. In its place the Information Governance Sub-committee will be formed with a remit to provide assurance that City is meeting its legal obligations. The sub-committee terms of reference were approved by the Executive Committee in 2016:

Information Governance Committee Terms of Reference

- To ensure that the Organisation has effective policies and management arrangements covering all aspects of Information Governance in line with the Organisation's overarching Information Governance Policy, i.e.

- Openness
- Legal Compliance
- Information Security
- Information Quality Assurance

- To ensure that the Organisation undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements.

- To establish an annual Information Governance Improvement Plan, secure the necessary implementation resources, and monitor the implementation of that plan.

- To receive and consider reports into: breaches of confidentiality and security, performance of the Organisation in respect of other legal targets e.g. FOI and Subject Access Requests, and where appropriate undertake or recommend remedial action.

- To report to the Executive Committee on Information Governance issues.

- To liaise with other Organisation committees, working groups and programme boards in order to promote Information Governance issues.

- The Group will meet a minimum of four times a year.

[redacted]
18/04/2017

Doc 2

Executive Committee are asked to **note** the progress of the working group.

Information Governance Working Group – Progress Report

In August 2015 the Executive Committee approved the formation of the Information Governance (I.G.) Working Group. This group had seven key objectives:

1. I.G. Sub-Committee reporting into Executive Committee (ExCo)
2. I.G. Role structure
3. I.G. Policy and framework
4. I.G. Staff training and awareness programme
5. University wide information discovery exercise and review
6. Information asset register and controls
7. I.G. audit method and schedule

The group was formed in January 2016 and has met each month along with our consultant [redacted] Considerable progress has been made however the method for identifying Information Asset Owners took longer than anticipated to agree. An approach to this objective was agreed in November and progress is now being made.

Update of objectives:

1. I.G. Sub-Committee reporting into Executive Committee (ExCo)

In July 2016 ExCo approved the formation of the I.G. Committee as a sub-committee of ExCo. This committee will start in 2017 after the first 6 months of asset identification.

2. I.G. Role descriptions and structure

As noted the original method of identifying Information Asset Owners took longer than anticipated to agree therefore they have not yet been asked to register their assets on the log. A revised method of identifying key information assets has now been agreed. This method will be by business processes, with the owners adding the assets to the register and then performing a risk assessment. This work will start in January.

3. I.G. Policy / framework

A draft I.G. Policy and framework has now been produced. This will be a 'living' document during the first 6 months of asset identification. The sub-committee will be asked to approve the Version 1.0 during the first meeting.

4. I.G. Staff training and awareness programme

Most Senior Information Risk Owners have now been trained. Online I.G. training has been developed in conjunction with [redacted] and is now available. ExCo approved making this training mandatory for all staff in July 2016. An awareness campaign has been planned and will start in February 2017 with the help of the newly identified Information Asset Owners. The online training will be launched at the start of the awareness campaign.

5. University wide information discovery exercise and review

All members of the I.G. Working Group have been asked to identify Assets in their schools and professional services following the approved method described above. Early in 2017 the assets will be entered on to the register and owners identified.

6. Information asset register and controls

The Information Asset register has been developed in SharePoint. It is ready for use early in 2017.

7. I.G. audit method and schedule

Initial conversations have taken place with internal audit and the first audit scheduled for September 2017

[redacted]
Information Services
19/12/2016

DPC2

Executive Committee are asked to **note** this report on the progress of the working group.

Information Governance Working Group – Progress Update

In August 2015 the Executive Committee (ExCo) approved the formation of the Information Governance (I.G.) Working Group. This group had seven key deliverables:

1. Creation of a I.G. Sub-Committee reporting into ExCo
2. I.G. Role structure defined
3. I.G. Policy and framework defined and implemented
4. Information Asset Owner training and awareness programme
5. University wide information discovery exercise and review of risks
6. Information asset register and controls defined and implemented
7. I.G. audit method and schedule agreed

In 2016 items one, two and three were completed also Senior Information Risk Owners (SIROs) were identified and trained. During March and June 2017 ninety Information asset owners (IAOs) have been identified across all schools and professional services. Thirty were trained in March and have now started to record their information assets. The second thirty were trained on the 14th June with the final training session scheduled for the 23rd June. Those who have received their training have started to identify and record their Information assets with City Law School and Finance having moved on to the risk assessment phase.

The following table shows progress on SIROs and IAOs identified, Information Assets logged in the register and risk assessments performed.

School / PS	SIRO	IAOs	Assets	Risk
Audit	1	1	[illegible]	[illegible]
Cass	1	9	[illegible]	[illegible]
CLS	1	7	38	16
DARO	1	2	3	0
Finance	1	3	14	14
Governance	1	3	[illegible]	0
Grad School	1	2	1	0
HR	1	4	[illegible]	0
IT	2	8	4	0
LEaD	1	[illegible]	[illegible]	0
Library	1	6	1	0
Marketing	1	5	1	0
PaF	1	6	1	0
Presidents Office	1	1	[illegible]	0
R&E	1	5	1	0
SaAS	[illegible]	7	3	0
SASS	1	8	16	0
SHS	1	6	1	0
SMCSE	1	4	[illegible]	0
SPPU	1	2	7	0
Grand Total	20	90	92	30

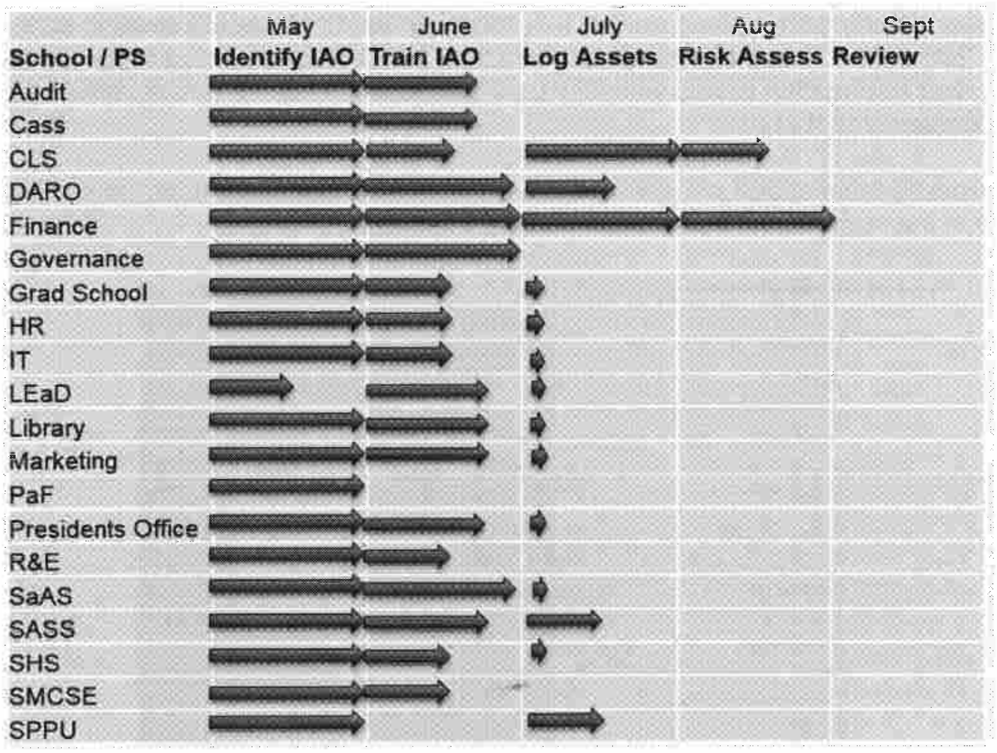
Table comments:

- SaAS is showing red for a SIRO as the previous SIRO ([redacted]) has left the University and her replacement has not yet been approached. This should be rectified in July.
- LEaD is showing red for IAO as having just one IAO is seen as being a risk. This should be rectified in July.
- Schools and Professional Services showing as red or amber for Assets have only just had or are waiting for their IAOs to be trained. All training will be complete by June 30th and progress in recording Information Assets will be monitored during July to ensure completion by July 31st.
- Finance and CLS have confirmed they have recorded all their information assets and both have made good progress in the risk assessments.

The key milestones are:

1. May 30st: Identify IAOs complete
2. June 31th: Train IAOs complete
3. July 30th: Record information assets complete
4. August 31st: Risk assessments complete
5. September 30th: Review all assets and risks
6. Q4/2017: First subcommittee meeting and risk report
7. Q1/2018: First audit

This table show progress against the milestones:



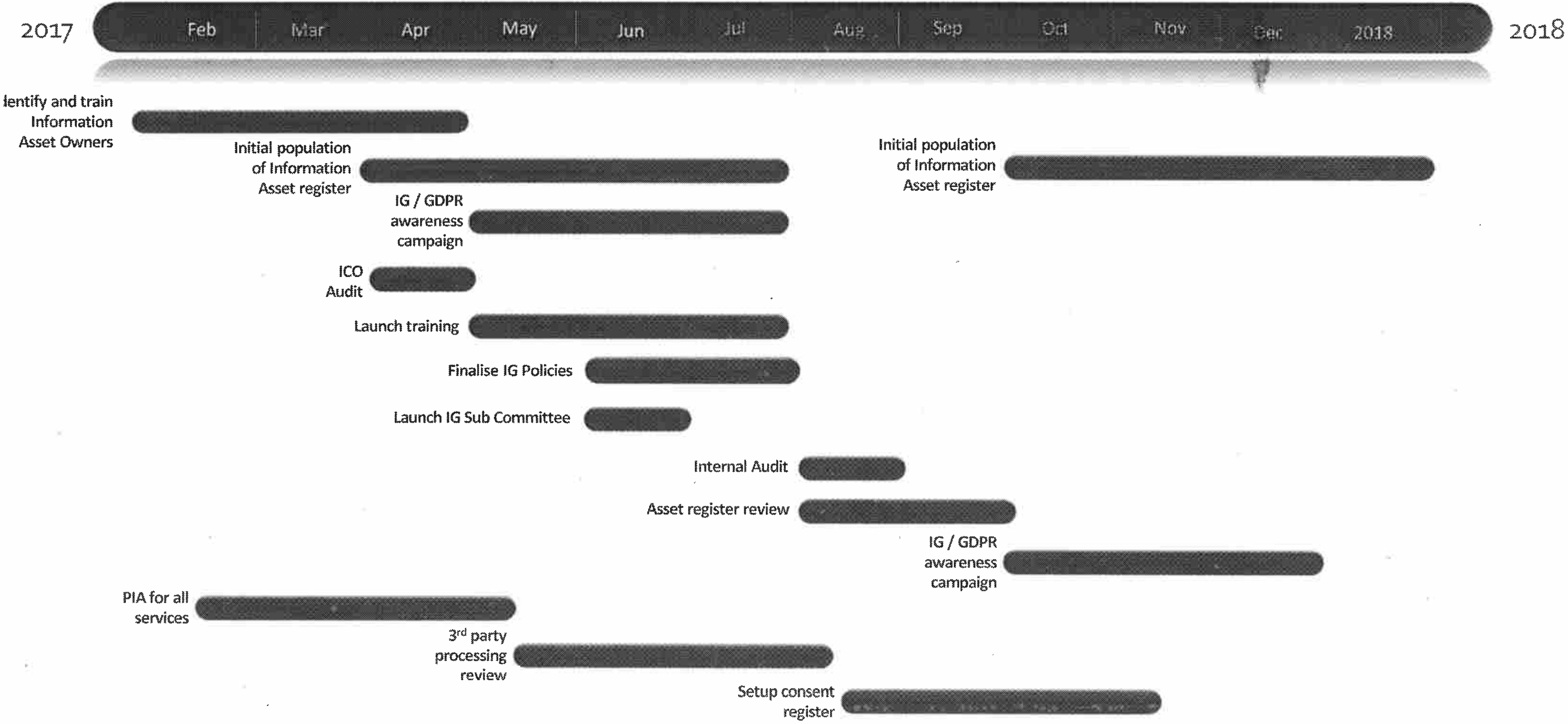
	May	June	July	Aug	Sept
School / PS	Identify IAO	Train IAO	Log Assets	Risk Assess	Review
Audit	→	→			
Cass	→	→			
CLS	→	→	→	→	
DARO	→	→	→		
Finance	→	→	→	→	
Governance	→	→			
Grad School	→	→	→		
HR	→	→	→		
IT	→	→	→		
LEaD	→	→	→		
Library	→	→	→		
Marketing	→	→	→		
PaF	→				
Presidents Office	→	→	→		
R&E	→	→			
SaAS	→	→	→		
SASS	→	→	→		
SHS	→	→	→		
SMCSE	→	→			
SPPU	→		→		

[redacted]

16/06/2017

DOC 3

Information Governance Group



Ientify and train Information Asset Owners

Initial population of Information Asset register

IG / GDPR awareness campaign

ICO Audit

Launch training

Finalise IG Policies

Launch IG Sub Committee

Internal Audit

Asset register review

Initial population of Information Asset register

IG / GDPR awareness campaign

PIA for all services

3rd party processing review

Setup consent register

Doc 4

SIRO	SIRO	SIRO	SIRO
Name	Position	School / PS	Date
Redacted	Dean	Grad School	42446
Redacted	ICM	IT	42446
Redacted	COO	SMCSE	42446
Redacted	COO	Cass	42465
Redacted	COO	CLS	42465
Redacted	COO	SHS	42465
Redacted	Sec	Governance	42465
Redacted	Director	DARO	42837
Redacted	Director	IT	42837
Redacted	COO	SASS	42837
Redacted	Dep. Director	Finance	
Redacted	Director	R&E	
Redacted	Ass. Director	SaAS	
Redacted	Director	SPPU	
Redacted	Dep. Director	HR	
Redacted	Director	Library	
Redacted	Dep. Director	Paf	
Redacted	Director	Marketing	
Redacted	Director	LEaD	
Redacted	Director	Presidents Office	
Redacted	Director	Audit Office	
IAO	**IAO**	**IAO**	**IAO**
Redacted	Chief Operating Officer	SASS	42801
Redacted	Executive Assistant to the Dean	SASS	42801
Redacted	Senior Course Officer	SASS	42801
Redacted	Quality Manager	SASS	42801
Redacted	Departmental Administrator	SASS	42801
Redacted	Head of Academic Services	SASS	42837
Redacted	Senior Lectuer & Divisional Lead	SHS	14/06/2017 13:30 - 16:30
Redacted	Lecturer	SHS	14/06/2017 13:30 - 16:30
Redacted	Programme Manager	SHS	23/06/2017 09:30 - 12:30

Redacted	Head of Academic Services	SHS	42801		
Redacted	Divisional Lead	SHS	42801		
Redacted	Senior Lecturer	SHS	42801		
Redacted	Professional Liaison Unit Manager	SMCSE	14/06/2017 13:30 - 16:30		
Redacted	P/G Course Operations Manager	SMCSE	23/06/2017 09:30 - 12:30		
Redacted	Undergraduate Course Operations Manager	SMCSE	23/06/2017 09:30 - 12:30		
Redacted	Head of Academic Services	SMCSE	42837		
Redacted	Planning & Performance Manager	SPPU	23/06/2017 13:30 - 16:30		
Redacted	Director	SPPU	42801		
MANAGEMENT VIEW	MANAGEMENT VIEW				
School / PS	SIRO	SIRO Trained	SIRO %	Nomitated IAOs	Expected I/
Audit		1	0	0	1	0
Cass		1	1	1	9	8
CLS		1	1	1	7	1
DARO		1	1	1	2	2
Finance		1	0	0	3	3
Governance		1	1	1	3	3
Grad School		1	1	1	2	1
HR		1	0	0	4	3
IT		2	2	1	8	8
LEaD		1	0	0	1	1
Library		1	0	0	6	4
Marketing		1	0	0	5	5
PaF		1	0	0	6	3
Presidents Office		1	0	0	1	0
R&E		1	0	0	5	5
SaAS		0	0	0	7	7
SASS		1	1	1	8	8
SHS		1	1	1	6	7
SMCSE		1	1	1	4	4
SPPU		1	1	1	2	2
Grand Total		20	5	0.6	90	14

Doc 6

GDPR – Changes to consent and Privacy Notices

Definition of consent:

The Directive requires the controller to provide "accurate and full information on all relevant issues," including the nature of the data that will be processed, the purposes of processing, the identity of the controller, and the identity of any other recipients of the data.

Data Controllers are required to provide the data subject with at least the following information:

- The identity and contact details of the data controller (or their representative) and where there is one, the data protection compliance officer.
- The purposes of the processing including the legitimate interests pursued by the data controller if that is one of the conditions for lawful processing relied upon to legitimise the processing.
- The period for which the personal data will be stored.
- Countries or organisations that the processor may transfer the data to and the level of protection afforded by that country.
- The source of the personal data if it has not been collected from the data subject themselves.
- Whether providing personal data is voluntary or obligatory and the possible consequences of not providing the information.
- Any other information necessary to guarantee the fair processing in respect of the data subject.
- Recipients or categories of recipients with whom the personal data are likely to be shared with.
- The data subjects' rights including: right of access to one's own personal data, right of correction, erasure and to object to processing, and the right to lodge a complaint with the ICO.

Consent had to be specific to the processing operations and the controller could not request open-ended or blanket consent to cover future processing

Under the GDPR, consent must be "freely given, specific, informed and unambiguous."

The GDPR gives data subjects the right to withdraw consent at any time and "it shall be as easy to withdraw consent as to give it." Controllers must inform data subjects of the right to withdraw before consent is given. Once consent is withdrawn, data subjects have the right to have their personal data erased and no longer used for processing.

Importantly, a controller may not make a service conditional upon consent, unless the processing is necessary for the service.

Third, the GDPR adds that consent must be specific to each data processing operation. However, the law exempts controllers from obtaining consent for subsequent processing operations if the operations are "compatible."

Additional processing for archiving in the public interest purposes or scientific and historical research generally will be considered compatible, and, therefore, exempt from specific consent.

To meet obligations set out under data protection laws on the fair processing of personal data businesses should only use data "in a way that people would reasonably expect" In addition, businesses must ensure "people know how their information will be used".

Doc 5

Data Protection Officers at City, University of London

Background

One of the requirements of the General Data Protection Regulations (GDPR) is that certain Data Controllers are required to appoint a Data Protection Officer (DPO). This applies to Data Controllers who fall into one or more of the following categories:

- if the processing is carried out by a public authority or body (irrespective of what data is being processed)
- if the core activities of the controller consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale
- if the core activities of the controller or consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences

All three apply to City, University of London (City) therefore we are required to appoint one or more.

The role and scope of the DPO

Responsibilities of a DPO

- Be the nominated officer on the Data Protection Register.
- Develop and implement the organisation's Data Protection Policy.
- Develop and implement privacy notice standards and templates
- Create 'best practice' guidance / review contracts for data processors
- Train and advise staff on the provisions of the Data Protection Act.
- Perform and review Privacy Impact Assessments ensuring suitable actions are identified
- Perform and review data breach responses ensuring suitable actions are identified
- Identify, review and monitor data processors, ensuring that they deal with data in a manner consistent with the 8 data protection principles.
- Process and respond to all requests for information by data subjects.
- Ensure data remains up-to-date and is destroyed when necessary.

Relevant skills and expertise required by the DPO include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- understanding of the processing operations carried out at City
- understanding of information technologies and data security
- knowledge of the Higher Education sector and how City operates
- ability to promote a data protection culture within City
- reports to the highest level of management at City (ExCo or Council)

The following resources should be provided to the DPO:

- active support of the DPO's function by ExCo
- sufficient time for DPOs to fulfil their tasks

- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff
- communication of the designation of the DPO to all staff
- continuous training

Several safeguards exist in order to enable the DPO to act in an independent manner:

- no instructions by City regarding the exercise of the DPO's tasks
- no dismissal or penalty by City for the performance of the DPO's tasks
- no conflict of interest with possible other tasks and duties

As far as protection impact assessments (PIAs) are concerned, City should seek the advice of the DPO, on the following issues, amongst others:

- whether or not to carry out a PIA
- what methodology to follow when carrying out a PIA
- what safeguards to apply to mitigate any risks to the rights and interests of the data subjects
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions are in compliance with data protection requirements

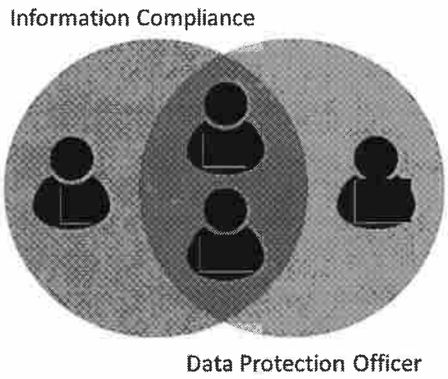
The DPO can be:

- A small team
- Exercised on the basis of a service contract
- Be external to an organisation

Suggested application at City

Option 1: Internal

Form a Data Protection Officer Matrix team wit[redacted] being the DPO supported by [redacted]



Responsibilities split:

[redacted]

- Be the nominated officer on the Data Protection Register.
- Develop the organisation's Data Protection Policy.
- Develop privacy notice standards and templates

- Review contracts for data processors
- Advise staff on the provisions of the Data Protection Act.
- Review Privacy Impact Assessments ensuring suitable actions are identified
- Review data breach responses ensuring suitable actions are identified

Information Compliance Team

- Perform Privacy Impact Assessments ensuring suitable actions are identified
- Perform data breach responses ensuring suitable actions are identified
- Train staff on the provisions of the Data Protection Act
- implement privacy notice standards and templates
- implement the organisation's Data Protection Policy
- Identify, review and monitor data processors, ensuring that they deal with data in a manner consistent with the 8 data protection principles.
- Process and respond to all requests for information by data subjects.
- Ensure data remains up-to-date and is destroyed when necessary.

Pros:

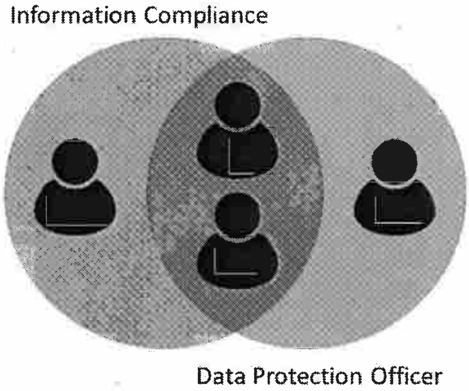
- William Jordan reports to the highest level of Management
- Line management remains with [redacted]
- [redacted] already correctly trained for this year

Cons

- Additional workload for [redacted] (0.2 FTE)
- Training needs to be updated at least every two years (~[redacted]

Option 2: External

Form a Data Protection Officer matrix team with an outsourced DPO supported by [redacted] and [redacted]



Responsibilities split:

Outsourced DPO:

- Be the nominated officer on the Data Protection Register.
- Develop the organisation's Data Protection Policy.

- Develop privacy notice standards and templates
- Review contracts for data processors
- Advise staff on the provisions of the Data Protection Act.
- Review Privacy Impact Assessments ensuring suitable actions are identified
- Review data breach responses ensuring suitable actions are identified

Information Compliance Team:

- Perform Privacy Impact Assessments ensuring suitable actions are identified
- Perform data breach responses ensuring suitable actions are identified
- Train staff on the provisions of the Data Protection Act
- implement privacy notice standards and templates
- implement the organisation's Data Protection Policy
- Identify, review and monitor data processors, ensuring that they deal with data in a manner consistent with the 8 data protection principles.
- Process and respond to all requests for information by data subjects.
- Ensure data remains up-to-date and is destroyed when necessary.

Pros:

- No additional workload
- External knowledge to guide GDPR activities
- Training webinars on demand
- No ongoing training requirements

Cons:

- Cost for service (First quote [redacted] per month)
- Need to upskill DPO on Citys working practices
- Need to interface with highest level of Management

[redacted]

07/06/2017