[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[redacted]	[illegible]	[redacted]	[illegible]	[redacted]

Questionnaire			Information and Guidance			
Question	Response	Response Comments	Question Guidance [illegible]	Corresponding Framework	Risk Score/Indicator	Critical
1 0 Information Systems [illegible]						
1 1 Does your organisation hold any of the following certifications relating to ICT systems used in the delivery of your service?			[illegible]	[illegible]		
a) Yes, Cyber Essentials [insert certificate number]	Yes	IASME-CE-0 3848				
b) Yes, Cyber Essentials Plus [insert certificate number]	No				5	
c) Yes, ICT systems are ISO 27001 certified [insert certificate number]	No	UC 10-0 RISCIS 38 visits UK to ensure in place accompliant solution called [illegible]			5	
1 2 A user access controls in place to ensure information stored on your ICT systems is only available [illegible]	Yes					
1 3 A acceptable use policies in force for all users and do they outline the rules for acceptable use of information assets?	Yes					
1 4 A policies and controls in place to ensure the following?						
Boundary protection is in place and always ensure the connection to an untrusted network	Yes					
Timely patching is applied against known vulnerabilities	Yes					
Systems are protected from malicious and mobile code	Yes					
Software and hardware are locked down to restrict unnecessary services	Yes					
A monitoring regime is in place to oversee how ICT systems are used	Yes					
Encryption of data in transit	Yes					
Encryption of data at rest	Yes					
1 5 Has the security of your ICT been evaluated through penetration testing or an IT Health Check during the last 12 months? If an email system has recently been upgraded, then please provide name of organisation.	Yes – Carried out by in email team	Project and departmental systems are tested by UCL ISD as needed, more details here https://www.ucl.ac.uk/informations-security/ technical advice/security-tips 1 2	[illegible]	[illegible]	5 - CHECK CREST or Tiger Scheme Scheme 5 Tiger Scheme 4 - Crest Organisation 3 - Cyber Essentials 0 - No	
2 0 Physical & Environmental [illegible]						
2 1 Has a review of the physical security risk been carried out within the last 12 months of the premises from which the solution will be supported supplied i.e. data centre, corporate offices?	Yes - and reviewed annually		[illegible]	[illegible]	3 - yes 0 - yes Annual view 0 - No	C Iced
3 0 Personnel & HR [illegible]						
3 1 A background verification check carried out on employees and contractors who have access to our assets?	Yes - but not to BPSS or BS 7858 Standard		[illegible]	[illegible]	3 - yes B, BS 3 - yes BS 0 - no enhanced enhanced 0 - No	C Iced
3 2 A organisational and individual responsibilities for information security clearly defined in the terms and conditions of employment contracts?	Yes		[illegible]	[illegible]	3 - yes 0 - No	C Iced
3 3 Do you have agreements with employees in place that will protect the department from supplier staff disclosing [illegible]	Yes			[illegible] - Information	3 - yes 0 - No	C Iced
3 4 Is a mechanism in place to ensure your employees and contractors receive appropriate information security awareness training upon appointment, and regular updates to organisational policies and procedures, as relevant for their job function?	Yes		[illegible]	[illegible] - Culture Awareness	3 - yes 0 - No	C Iced
4 0 Organisation [illegible]						
4 1 Is there a senior individual within your organisation who is responsible for security policy?	Yes - please provide contact details	[redacted]	[illegible]	[illegible] - Governance	3 - yes 0 - No	C Iced
5 0 Security Policy [illegible]						
5 1 Do you have a formally documented information security policy setting out your organisation's overall approach to protecting valuable assets that has been approved by management, is communicated to all staff, [illegible]	Yes		[illegible]	[illegible] - Risk Management	3 - yes 0 - No	C Iced
6 0 Asset Management [illegible]						
6 1 Do you have policies in place which detail how our assets should be;			[illegible]	[illegible] - Information		
handled	Yes					C Iced No
copied	Yes					C Iced No
stored	Yes					C Iced No
transmitted	Yes					C Iced No
destroyed	Yes					C Iced No
returned	Yes					C Iced No
7 0 Incident Management [illegible]						
7 1 Do you have policies in place which set out how information security incidents, and breaches to the confidentiality of data, should be managed and to whom should they be escalated?	Yes		[illegible]	[illegible] - [illegible]	3 - yes 0 - No	C Iced
7 2 In the event of a loss or breach of one of our assets which of the following actions would your organisation [illegible]	Report the incident to the Department			[illegible] - [illegible]	4 - Reactively each 3 - Date reference 0 - Reactive Ind	
8 0 Business Continuity [illegible]						
8 1 Does your organisation have business continuity and disaster recovery plans in place to maintain or quickly resume any services you provide or use?	Yes		[illegible]	[illegible] - [illegible]	3 - no company BS 3 - yes 0 - No	C Iced
9 0 Compliance [illegible]						
9 1 Does your company provide guidance to staff on handling our information with respect to the following legislation;			[illegible]	[illegible] - Culture and Awareness		
Data Protection Act/General Data Protection Regulation (GDPR)	Yes					
Freedom of Information	Yes					
10 0 Supplier Relationships [illegible]						
Do you use sub contractors in the delivery of your service?	Yes				[illegible]	
10 2 Does your company gain assurance that your sub-contractors and any other delivery partners or third-party suppliers are compliant with your security policies by delegating information security requirements in contracts?	Yes		[illegible]	[illegible] - Risk Management	3	C Iced