Updated: November 2021

Information Security Policy for US Title IV federal aid program

UCL is required by the Gramm-Leach-Bliley Act (GLBA) to implement its regulations as detailed in Dear Colleague Letters GEN-15-18 and GEN-16-12. UCL is committed to protecting the information of its students and has set up the UCL Information Security Group to help both staff and students manage their responsibilities when it comes to looking after their own and UCL's information.

Designated individual for the information security program	**Sarah Lawson, Chief Information Security Officer, UCL** **E:** sarah.j.lawson@ucl.ac.uk

#	***Safeguard***	**Controls**
1.	Documented policy framework around IT and system security:	UCL's main Information Security Policy can be accessed at: ***https://www.ucl.ac.uk/information-security/information-security-policy*** Other relevant information security policies are also available at the link above.
2.	Employee training and management	UCL staff and students have to undertake the Information Security Awareness Course. See here for details: ***https://www.ucl.ac.uk/information-security/information-security-awareness-course***
3.	Risk assessment	Risk Assessments are carried out on all systems that hold personal information. UCL has a comprehensive Risk Management and Compliance program in place. See here for details: ***https://www.ucl.ac.uk/information-security/information-risk-management-and-compliance***
4.	Information systems, including network and software design, as well as information processing, storage, transmission, and disposal	UCL has formal processes for the design, implementation and maintenance of its information systems, including its network and software design. Additionally, UCL has policies (see pt. 2) above and guidance in place for its information processing, storage, transmission and disposal of its information assets.
5.	Detecting, preventing, and responding to attacks, intrusions, or other system failures	UCL has put in place relevant infrastructure to ensure that its information assets are protected. Some of these include: Firewalls (where necessary), a Security Information and Event Management (SIEM) tool, Antivirus and Full-Disk Encryption (where necessary). All key systems are regularly monitored by industry standard IT Monitoring and management tools.
6	Access to US systems	All US Loans systems require two factor authentication (TFA) – password and additional numeric code. Passwords must be at least 12 characters long with a mix of letters, numbers and special characters, and the security code is generated from a portable token key issued by the US to authorised individuals.

Signed: SJLawson

Dated: 21st December 2021