LONDON'S GLOBAL UNIVERSITY

UCL Data Safe Haven
Acceptable Use Statement

UCL Computing Regulations are based on the premise that access to resources is generally forbidden unless expressly permitted.

You are reminded that the UCL Information Security Policy, Data Protection Policy and Computing Regulations are contractually mandated

The UCL Data Safe Haven is a secure service that through various Standard Operating Procedures (SOPs) supports the secure storage and exchange of sensitive personal data.

In using the Data Safe Haven I agree:

- To comply with all relevant standard operating procedures and policies in relation to my use of the Data Safe Haven
- My use of the Data Safe Haven will be for UCL's authorised business and those resources and functions allocated to me by authorised personnel. Any other activity including but not limited to the use of offensive material is forbidden
- UCL reserves the right to monitor and audit the use of the Data Safe Haven
- To report any information security incidents promptly in accordance with the UCL Information Security Group incident procedure
- The transfer and sharing of personal sensitive data must respect the rights of research data subjects
- Use of the Data Safe Haven for any illegal activity will be grounds for disciplinary action
- To act responsibly at all times and not put Data Safe Haven resources and sensitive data at risk.
- I will not attempt to circumvent the security measures implemented within the Data Safe Haven. This includes, but is not limited to, taking screenshots and sharing of credentials.
- I will ensure that the 'token' I have been issued with is stored and treated with the same level of security as a password.

- To ensure that any working environment when using the Data Safe Haven is chosen to prevent unauthorised access to information eg. through ‘shoulder surfing’ and screens will be positioned to face away from windows.

I fully understand my responsibilities for use of the Data Safe Haven and what constitutes a breach of the UCL Computing Regulations, UCL SLMS Information Governance Policy, UCL Data Protection Policy and UCL Information Security Policy.

I have completed UCL approved Information Governance training for my use of confidential UCL information assets. I acknowledge acceptance of my responsibilities for confidential information assets by signing this declaration form below.

Signature: ……

Name (CAPITALS): ……

Job Title: ....…….....

Date: ……..

Mandated UCL policies:

UCL Computing Regulations:
https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Regulations
UCL Data Protection Policy:
https://www.ucl.ac.uk/information-security/sites/information-security/files/data-protection.pdf
UCL Information Security Policy:
https://www.ucl.ac.uk/information-security/sites/information-security/files/policy.pdf
UCL Information Security Incident Reporting Procedure
https://www.ucl.ac.uk/information-security/technical-advice/incident-response

SLMS IG Framework documents:

UCL SLMS-IG03 Information Governance Policy:
https://www.ucl.ac.uk/isd/sites/isd/files/slms-ig03_research_information_governance_policy.pdf