AIMHIGHER LONDON LIMITED

Data security policy

1. This policy

1.1 This policy sets out the measures Aimhigher London Limited (registered office: The Granary, Brewer Street, Bletchingley, Surrey, RH1 4QP, company number: 07859881) ("the Company") will take and practices all employees, contractors and other staff ("Users") should follow in respect of the use of computer systems, software, hardware, devices and other IT infrastructure ("Systems").

1.2 The measures and practices described in this policy are designed to ensure that the Systems are secure and protected against internal and external threats.

1.3 In following this policy, Users should pay particular attention to anything that relates to or may include personal data and the processing of such data.

1.4 This policy should be read in conjunction with Company's Privacy Policy and internal Data Protection Policy.

1.5 Users should not use the Systems until they have read this policy.

1.6 The current Data Protection Manager is Suzanne Marchment, who may be contacted at S.Marchment@kingston.ac.uk

2. Software

2.1 Users must not install or download any software without the express approval of your line manager ("Line Manager"). .

2.2 All software installation must be carried out by or with the approval of the Data Protection Manager. Any software downloaded should be from an authorised, recognised source and should be subject to virus scans before the software is operated or installed.

2.3 Users must comply with all instructions of your Line Manager and relevant technical staff in respect of updates, installations and changes to software which may include allowing technical staff to access their device for a period.

2.4 If a User suspects that any software has a defect or has become corrupted or may in some other way present a risk to the security and integrity of the Systems then they must notify their Line Manager immediately.

2.5 Aimhigher will regularly monitor and consider the software requirements of the business to ensure that it is using the most up-to-date or appropriate versions of all relevant programs and applications.

3. Hardware

3.1 Desktop devices and other physical parts of the systems will be located in a safe and secure environment which is only accessible by Users and other authorised people.

3.2 All desktop devices and other physical parts of the Systems will, where practicable, be held securely and in such a manner as to reduce the risk of damage or theft.

3.3 Desktop devices must be protected if possible with a password protected screensaver or lock-out mechanism.

3.4 All other hardware that is not ordinarily used by Users such as servers must be kept in a safe and secure environment and such hardware is only accessible by such members of staff as is necessary for the proper functioning of the Systems.

3.5 If a User suspects that any hardware has a defect or has become corrupted or may in some other way present a risk to the security and integrity of the Systems then they must notify their Line Manager immediately.

3.6 Users must not use or insert removable media received from third parties without the approval of their Line Manager. The Line Manager may require a User to provide them with removable media so that they can access the contents securely.

4. Mobile devices

4.1 All mobile devices (including phones, laptops and tablets) must be transported safely and securely and should be treated with due care and attention at all times.

4.2 Mobile devices should not be left unattended at any time and must be stored safely overnight when at a User's home or otherwise not on Company premises.

4.3 Mobile devices must be locked when not in use and only accessible by password.

4.4 If a User suspects a mobile device has been accessed by or tampered with by another person they must notify their Line Manager as soon as they become aware of such unauthorised use.

4.5 Users will comply with all requirements of their Line Manager in respect of mobile devices and may be required to return or replace such devices at any time.

4.6 Data should not be transferred or accessed on any mobile device unless the device is securely password protected in accordance with this policy.

5. Passwords

5.1 All Systems will be password-protected.

5.2 Each user will be responsible for creating appropriate secure passwords to enable them to access the Systems. Users may be required to create different passwords for different devices and parts of the Systems.

5.3 Passwords must be at least six characters long, non-obvious, contain a mixture of letters, numbers and symbols and (if possible) combine lower and upper case letters.

5.4 Passwords should be changed regularly and in any event every three months.

5.5 Users must not share their passwords with any other person and must not record them anywhere in writing (either physically or electronically). If a User forgets a

password they must contact their Line Manager or technical staff to resolve the issue and enable them to access the Systems again.

5.6 All devices must be set to lock when they are not in use and must be set up so that they can only be accessed by entering the relevant password each time they are used.

5.7 Data stored by Company will be password protected and encrypted with strong encryption.

6. Account Management

6.1 This policy refers to two kinds of Systems user accounts – "standard accounts" and "systems accounts".

6.2 All accounts are under the supervision and management of our technical staff .

6.3 On first login to a new account, the user must change the default password (if any).

6.4 Users may not share login details with any other user, and accounts may not be used by more than one member of staff or as a generic account.

6.5 Aimhigher shall conduct regular reviews of all accounts (both standard accounts and systems accounts) to ensure that the account users, permissions and levels of access granted remain secure, appropriate and in line with business need. Such reviews shall occur not less than once every 90 days.

Standard Accounts

6.6 Employees and staff working with Company may be given access to various accounts and logins including a network account, an email account, accounts with business-related SaaS providers and may also be given access to certain shared drives and information – these are referred to as "standard accounts".

6.7 When a team member joins Company they will be given access to standard accounts. Access to standard accounts may also be granted from time to time to existing staff members.

6.8 Standard accounts must be deactivated when a staff member leaves and accounts may only remain active for the period needed for that staff member to fulfil the relevant need.

6.9 Users are not permitted to access their accounts after leaving Company. Systems will be put in place by Aimhigher to ensure that accounts are deactivated when staff leave Company.

Systems Accounts

6.10 Technical staff may be given access to more privileged and secure accounts including systems or network administrator accounts or accounts which allow for services or systems used by Company to be managed – these are referred to as "systems accounts". Any account which allows a user to access any back-end Systems or change any settings for another user or standard account will be deemed to be a systems account.

6.11 Access to systems accounts may only be granted by the directors of Aimhigher and may be withdrawn at any time.

6.12 Systems accounts must be reviewed periodically to ensure that levels of access and permission remain appropriate. Systems accounts must be withdrawn if they are no longer required or if the relevant staff member no longer needs access to the account.

6.13 Systems accounts must be operated by users only for the agreed and intended purposes, must be separately from standard accounts which are operated by the same users.

6.14 No systems accounts may be accessed using a default username or password and any default usernames or passwords must be changed at the earliest opportunity.

6.15 Systems accounts must not be used to attempt to or gain access to Systems and information that the user does not have authority or a proper purpose to access.

7. Personal data

7.1 The Company has various statutory obligations in relation to personal data, including under the General Data Protection Regulation (as directly effective or as otherwise implemented into UK law). Users must only process personal data in accordance with the Company Data Protection Policy (which may be updated from time to time), this policy and all other instructions in respect of the handling of personal data.

7.2 All personal data must be stored securely using passwords, encryption or such other technological and security measures that the Data Protection Manager deems necessary and appropriate.

7.3 Personal data must only be transferred onto removable electronic media (including USB sticks and CDs) when strictly necessary and with the approval of the Data Protection Manager . Any such removable electronic media containing personal data must be password protected and handled and transported safely and securely at all times.

8. Breach

8.1 If a User becomes aware of a breach of the Systems or suspects that a breach has occurred or is about to occur then they must notify the Data Protection Manager immediately.

8.2 Users must follow all instructions of Aimhigher and their Line Manager and will provide all necessary assistance to address a breach as soon as practicable.

8.3 If a User learns of a suspected or actual personal data breach, it must be immediately reported to the Data Protection Manager. The report should include full details of the incident, when the breach occurred (dates and times), the nature of the information concerned, and how many individuals are involved.

8.4 The Data Protection Manager will perform an internal investigation and take appropriate remedial measures in a timely manner.

8.5 Users must not attempt to address a breach of the Systems or a data breach on their own and without notifying their Line Manager and the Data Protection Manager in accordance with this policy.

9. Hosting Partners

9.1 From time to time our Systems may be hosted by a partner organisation ("Hosting Partner").

9.2 The Hosting Partner as at the date of this Data Security Policy is Kingston University (IT Security Policy; Information Security Policy).

9.3 All Users should review the data protection and data security documents and policies of any Hosting Partner when they are provided to them.

9.4 All Users are required to comply with the Hosting Partners data security documents and policies as appropriate and necessary.

9.5 If any User have any concern regarding the Hosting Partner and their data protection and data security documents and policies, these should be reported to the Data Protection Manager as soon as possible.