

1. Introduction

This document sets out the measures to be taken by all employees of Cavendish Consulting Limited, 8-10 Mansion House Place, London, EC4N 8BJ. (Cavendish) and by Cavendish as a whole in order to protect its computer systems, devices, infrastructure, computing environment and any and all other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate, or accidental.

2. Key Principles

- 2.1 All IT Systems are to be protected against unauthorised access.
- 2.2 All IT Systems are to be used only in compliance with relevant Company Policies.
- 2.3 All employees of Cavendish and any and all third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors (collectively, "Users"), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.
- 2.4 All line managers must ensure that all Users under their control and direction must adhere to and comply with this Policy at all times as required under paragraph 2.3.
- 2.5 All data stored on IT Systems are to be managed securely in compliance with all relevant parts of EU Regulation 2016/679 General Data Protection Regulation ("GDPR") and all other laws governing data protection whether now or in the future in force.
- 2.6 All data stored on IT Systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data, and confidential information). All data so classified must be handled appropriately in accordance with its classification.
- 2.7 All data stored on IT Systems shall be available only to those Users with a legitimate need for access.
- 2.8 All data stored on IT Systems shall be protected against unauthorised access and/or processing.
- 2.9 All data stored on IT Systems shall be protected against loss and/or corruption.
- 2.10 All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by a dedicated external representative or Cavendish internal IT Department or by such third party/parties as the IT Department may from time to time authorise.
- 2.11 The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the IT Department unless expressly stated otherwise.
- 2.12 All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the IT Department. Any breach which is either known or suspected to involve personal data shall be reported to the Company Data Protection Representative.

- 2.13 All Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the IT Department. If any such concerns relate in any way to personal data, such concerns must also be reported to the Company Data Protection Representative.

3. IT Department Responsibilities

- 3.1 The Head of IT shall be responsible for the following:

ensuring that all IT Systems are assessed and deemed suitable for compliance with Cavendish's security requirements;

- a) ensuring that IT security standards within Cavendish are effectively implemented and regularly reviewed, working in consultation with Cavendish's senior management and Company Data Protection Representative, as appropriate, and reporting the outcome of such reviews to Cavendish's senior management.
- b) ensuring that all Users are kept aware of the requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the Cyber Essentials Plus, GDPR and the Computer Misuse Act 1990.

- 3.2 The IT Staff shall be responsible for the following:

- a) assisting all Users in understanding and complying with this Policy;
- b) providing all Users with appropriate support and training in IT security matters and use of IT Systems.
- c) ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements.
- d) receiving and handling all reports relating to IT security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing the Company Data Protection Representative.
- e) taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness.
- f) assisting the Head of IT in monitoring all IT security within Cavendish and taking all necessary action to implement this Policy and any changes made to this Policy in the future; and
- g) ensuring that regular backups are taken of all data stored within the IT Systems servers at intervals no less than 12 hours and that such backups are stored at a suitable location onsite and offsite. All backups should be encrypted using AES 256.

4. **Users' Responsibilities**

- 4.1 All Users must comply with all relevant parts of this Policy at all times when using the IT Systems.
- 4.2 All Users must use the IT Systems only within the bounds of UK law and must not use the IT Systems for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.
- 4.3 Users must immediately inform the IT Department (and, where such concerns relate to personal data, the Company Data Protection Representative) of any and all security concerns relating to the IT Systems.
- 4.4 Users must immediately inform the IT Department of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.
- 4.5 Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under Cavendish's disciplinary procedures.

5. **Software Security Measures**

- 5.1 All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) will be kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases will be applied at the sole discretion of the IT Department. This provision does not extend to upgrading software to new 'major releases' (e.g. from version 1.0 to version 2.0), only to updates within a particular major release (e.g. from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release, falling within the remit of new software procurement and outside the scope of this provision.
- 5.2 Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied. If the security flaw affects, is likely to affect, or is suspected to affect any personal data, the Company Data Protection Representative shall be informed immediately.
- 5.3 No Users may install or purchase any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the Head of IT. This includes SaaS (Software as a Service) and cloud platforms. Any software belonging to Users must be approved by the IT Department and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.
- 5.4 All software will be installed onto the IT Systems by the IT Department unless an individual User is given written permission to do so by the Head of IT. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

6. **Anti-Virus Security Measures**

- 6.1 All IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall, and other suitable internet security software. All such software will be kept up-to-date with the latest software updates and definitions.
- 6.2 All IT Systems protected by anti-virus software will be subject to a full system scan at least once a week.
- 6.3 All physical media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred. Such virus scans shall be performed automatically upon connection / insertion of media, by the User or by the IT Staff / Manager.
- 6.4 Users shall be permitted to transfer files using cloud storage systems only with the approval of the Head of IT. All files downloaded from any cloud storage system must be scanned for viruses during the download process. This will be an automatic process performed by the antivirus software.
- 6.5 Any files being sent to third parties outside Cavendish, whether by email, on physical media, or by other means (e.g. shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate. All email attachments are scanned automatically upon sending.
- 6.6 Where any virus is detected by a User this must be reported immediately to the IT Department (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or device will be provided immediately or within 24 hours if no replacement is available at Cavendish's satellite offices to limit disruption to the User.
- 6.7 If any virus or other malware affects, is likely to affect, or is suspected to affect any personal data, in addition to the above, the issue must be reported immediately to the Company Data Protection Representative.
- 6.8 Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under Cavendish's disciplinary procedures.

7. **Hardware Security Measures**

- 7.1 Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised access to such locations for any reason.

- 7.2 All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) shall be located, wherever possible and practical, in secured, climate-controlled rooms and/or in locked cabinets which may be accessed only by designated members of the IT Department.
- 7.3 No Users shall have access to any IT Systems not intended for normal use by Users (including such devices mentioned above) without the express permission of the Head of IT. Under normal circumstances, whenever a problem with such IT Systems is identified by a User, that problem must be reported to the IT Department. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the Head of IT.
- 7.4 All non-mobile devices (including, but not limited to, desktop computers, workstations, and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.
- 7.5 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided Cavendish should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended, they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes. If any such mobile device is to be left in a vehicle it must be stored out of sight and, where possible, in a locked compartment. Under no circumstances should devices be taken to private social events, which includes company functions unless the user is exercising the duties of their position for which a device is required. Failure to observe this requirement will constitute a disciplinary offence.
- 7.6 The IT Department shall maintain a complete asset register of all IT Systems. All IT Systems shall be labelled, and the corresponding data shall be kept on the asset register.

8. Access Security

- 8.1 Access privileges for all IT Systems shall be determined on the basis of Users' levels of authority within Cavendish and the requirements of their job roles. Users shall not be granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.
 - 8.1.1 Administrative access to devices will only be granted dependent on the Users job role and at the discretion of the Head of IT. If a User is granted administrative access to their local device they must not download, install or subscribe to software without the express permission from the Head of IT. Failure to observe this requirement will constitute a disciplinary offence.
- 8.2 All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or

such other form of secure log-in system as the IT Department may deem appropriate and approve. Not all forms of biometric log-in are considered secure. Only those methods approved by the IT Department may be used.

- 8.3 All passwords must, where the software, computer, or device allows:
- a) be at least 7 characters long;
 - b) contain a combination of at least 1 uppercase letter, 1 number, and 1 special character;
 - c) be changed at least every 365 days;
 - d) be different from the previous password.
 - e) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc); and
 - f) be created by individual Users or system generated.
- 8.4 Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone, including the Head of IT and the IT Staff. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password, they should change their password immediately and report the suspected breach of security to the IT Department and, where personal data could be accessed by an unauthorised individual, the Company Data Protection Representative.
- 8.5 If a User forgets their password, this should be reported to the IT Department. The IT Department will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.
- 8.6 Users should not write down passwords if it is possible to remember them. If a User cannot remember a password, it should be stored securely (e.g. in a locked drawer or in a secure password database) and under no circumstances should passwords be left on display for others to see (e.g. by attaching a note to a computer display).
- 8.7 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after 5 minutes of inactivity. This time period cannot be changed by Users and Users may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).
- 8.8 Where a device is to be left unattended for any period of time, the User must lock the device (and screen where appropriate) before leaving it. Failure to observe this requirement will constitute a disciplinary offence.
- 8.9 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by Cavendish shall be set to lock, sleep, or similar, after 5 minutes of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake, or similar. Users may not alter this time period.

- 8.10 Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the Head of IT. Any such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared by the Head of IT and, where such access renders personal data accessible by the outside party, the Company Data Protection Representative.
- 8.11 Users may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the Cavendish Guest WiFi only subject to the approval of the IT Department. Any and all instructions and requirements provided by the IT Department governing the use of Users' own devices when connected to Cavendish network must be followed at all times. Users' use of their own devices shall be subject to, and governed by, all relevant Company Policies (including, but not limited to, this Policy) while those devices are connected to Cavendish network or to any other part of the IT Systems. The IT Department shall reserve the right to request the immediate disconnection of any such devices without notice.

9. **Data Storage Security**

- 9.1 All data, and in particular personal data, should be stored securely using passwords.
- 9.2 All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.
- 9.3 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Cavendish or otherwise without the formal written approval of the Company Data Protection Representative and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary. This includes synchronising data to a mobile device from Cavendish's Office365 Tenancy. Failure to observe this requirement will constitute a disciplinary offence.
- 9.4 No data, and in particular personal data, should be transferred to any computer or device personally belonging to a User unless the User in question is a contractor or sub-contractor working on behalf of Cavendish and that User has agreed to comply fully with Cavendish's Data Protection Policy and the GDPR.
- 9.5 No data, and in particular personal data, should be transferred to any third-party cloud-based storage, for example DropBox, Google Drive etc, without the express permission of the Head of IT and the Managing Director, whether the service has been set up with a User's Cavendish email address or personal e-mail address. Failure to observe this requirement will constitute a disciplinary offence.
- 9.6 Personal data must only be stored on Cavendish's Office365 Tenancy or using other cloud-based database services authorised by the Head of IT, in accordance with procedures set out in the "Data Protection Process & Procedure Manual". Failure to observe these requirements will constitute a disciplinary offence.

10. Data Protection

- 10.1 All personal data (as defined in the GDPR) collected, held, and processed by Cavendish will be collected, held, and processed strictly in accordance with the principles of the GDPR, the provisions of the GDPR and Cavendish's Data Protection Policy.
- 10.2 All Users handling data for and on behalf of Cavendish shall be subject to, and must comply with, the provisions of Cavendish's Data Protection Policy at all times. In particular, the following shall apply:
- a) All emails containing personal data must be encrypted, this is done automatically;
 - b) All emails containing personal data must be marked "confidential";
 - c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;
 - d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
 - e) Personal data contained in the body of an email, whether sent or received, should be copied directly from the body of that email, and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted this will be carried out by a weekly automated task;
 - f) All personal data to be transferred physically, including that on removable electronic media, shall be transferred in a suitable container marked "confidential".
 - g) Where any confidential or personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the User must lock the computer and screen before leaving it.
- 10.3 Any questions relating to data protection should be referred to the Company Data Protection Representative.

11. Internet and Email Use

- 11.1 All Users shall be subject to, and must comply with, the provisions of Cavendish's Communications, Email and Internet Policy when using the IT Systems.
- 11.2 Where provisions in this Policy require any additional steps to be taken to ensure IT security when using the internet or email over and above the requirements imposed by the Communications, Email and Internet Policy, Users must take such steps as required.

12. Reporting IT Security Breaches

- 12.1 Subject to paragraph 12.2, all concerns, questions, suspected breaches, or known breaches shall be referred immediately to the IT Department or the Head of IT.

- 12.2 All concerns, questions, suspected breaches, or known breaches that involve personal data shall be referred immediately to the Company Data Protection Representative who shall handle the matter in accordance with Cavendish's Data Protection Policy.
- 12.3 Upon receiving a question or notification of a breach, the IT Department shall, within 24 hours, assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps as the IT Department deems necessary to respond to the issue.
- 12.4 Under no circumstances should a User attempt to resolve an IT security breach on their own without first consulting the IT Department (or the Company Data Protection Representative, as appropriate). Users may only attempt to resolve IT security breaches under the instruction of, and with the express permission of, the IT Department.
- 12.5 All IT security breaches, whether remedied by the IT Department or by a User under the IT Department's direction, shall be fully documented.

13. **Policy Review**

The Company shall review this Policy not less than annually and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. All questions, concerns, and other feedback relating to this Policy should be communicated to the Head of IT and the Company Data Protection Representative.

14. **Commitment to Improvement**

It is the policy of Cavendish to commit to continually improve and maintain an Information Security Management System designed to meet the requirements of ISO27001:2013 in pursuit of its primary objectives.

15. **Implementation of Policy**

This Policy shall be deemed effective as of 26th June 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

16. **Data Protection Contact**

Data Protection Representative: David Loten, Finance Development Manager

Email address: dataprotection@cavendishconsulting.com

Telephone number: 01962 893 893

Postal Address: 8-10 Mansion House Place, London, EC4N 8BJ.