

# CAST COMMERCIAL ACUMEN LIMITED

## Information and Data Security Policy

### 1. Introduction

- 1.1. This document sets out the measures to be taken by all employees, contractors and associates of Cast Commercial Acumen Limited (the “Company”) and by the Company as a whole in order to protect information and data (electronic and otherwise) collected, held, and processed by the Company, and to protect the Company’s 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.
- 1.2. For the purposes of this Policy, the terms “information” and “data” are interchangeable and shall refer to the following type(s):
- a) **Business Information** meaning any of the Company’s business-related information other than Personal Data about customers, clients, suppliers, and other business contacts.
  - b) **Confidential Information** meaning any trade secrets, intellectual property, or other Confidential Information (belonging to the Company or third parties) processed by the Company.
  - c) **Personal Data** meaning any information that relates to an individual who can be identified from the information, either directly or indirectly as detailed in 1.4 below.
  - d) **Sensitive Personal Data** meaning information about an individuals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership) health, sex life, sexual orientation, genetic information, or biometric information (where this is used to identify an individual).
- 1.3. This Policy shall be subject to, and interpreted in accordance with, the Data Protection Legislation. “Data Protection Legislation” means all legislation and regulations in force from time to time regulating the use of Personal Data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the “UK GDPR”), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.
- 1.4. For the purposes of this Policy, “Personal Data” shall carry the meaning defined in Article 4 of the UK GDPR: any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

## 2. Roles and responsibilities

- 2.1 All employees, contractors and associates have a responsibility for information security. The Company Data Protection Officer (DPO) has overall responsibility for this policy, specifically they must:
- a) Implement and maintain this policy.
  - b) Monitor potential threats and actual security breaches.
  - c) Ensure employees, contractors and associates are aware of their responsibilities in relation to information security and confidentiality.
  - d) Ensure compliance with the UK GDPR and all other relevant legislation and guidance.

## 3. Scope of this policy

- 3.1 This policy covers all written, verbal, and digital information held, used, or transmitted by or on behalf of the Company irrespective of media. This includes, but is not limited to:
- a) Paper records.
  - b) Hand-held devices.
  - c) Telephones (landline and mobile).
  - d) Information stored on computer systems.
  - e) Information stored on cloud systems.
  - f) Information passed verbally.
- 3.2 The information covered by this policy may include:
- a) Personal Data relating to employees, customers, clients, contractors, associates, and other business contacts.
  - b) Other business information
  - c) Confidential Information .
- 3.3 This policy supplements the Company's Data Protection Policy and all other policies relating to data protection, internet, email, social media, communications, and document retention. The content of these policies must be considered and taken into account alongside this policy.

#### 4. **General Principles**

- 4.1 All information must be:
  - a) Treated as commercial valuable, and
  - b) Protected from loss, theft, misuse and inappropriate access or disclosure.
- 4.2 Through the use of appropriate technical and organisational measures all Personal Data, including sensitive Personal Data, must be protected against:
  - a) Unauthorised and / or unlawful processing, and
  - b) Accidental loss, destruction, or damage
- 4.3 All information, apart from Personal Data is owned by the Company and not by an individual or team.
- 4.4 Any information must only be used in connection with work being undertaken by the Company. It must not be used for any other personal or commercial purposes.
- 4.5 Any Personal Data must only be processed for the specified, explicit, and legitimate purpose for which it is collected.

#### 5. **Information Management**

- 5.1 Any Personal Data must be processed in accordance with:
  - a) The data protection principles
  - b) The Company policies on data protection
  - c) The Company's other relevant policies
- 5.2 All Personal Data collected, used, and stored must by:
  - a) Adequate, relevant, and limited to what is necessary for the relevant purposes, and
  - b) Kept accurate and up to date.
- 5.3 The Company will take appropriate technical and organisational measures to ensure that Personal Data is kept secure against unauthorised or unlawful processing and against accidental loss, destruction, or damage. These measures include:
  - a) The encryption of Personal Data
  - b) The pseudonymisation of Personal Data
  - c) Dual factor authentication
  - d) The use of strong passwords
- 5.4 Any Personal Data and Confidential Information must not be kept any longer

than is necessary and will be stored and destroyed in accordance with the Data Retention Policy.

## 6. Access to Information

- 6.1 All documents containing and any equipment displaying Confidential Information should be placed and positioned so that anyone passing by cannot see them (e.g., through office windows or glass doors)
- 6.2 Any visitors must not be left alone in areas or situations where they may have access to Confidential Information .
- 6.3 All paper documents, back-up systems and devices containing Confidential Information must be securely locked away:
  - a) Whenever desks are unoccupied, and
  - b) At the end of the working day.

## 7. Communications and transfer of information

- 7.1 When speaking in public places (e.g., when speaking on a mobile phone) employees, contractors, and associates must take care in maintaining confidentiality.
- 7.2 Confidential Information must be marked 'strictly private and confidential' and circulated only to those who need to know the information in the course of their work.
- 7.3 Confidential Information must not be removed from the Company offices (and systems) unless required for authorised business purposes and then only in accordance with the subsequent paragraph.
- 7.4 If the removal of Confidential Information from the Company's offices is permitted all reasonable steps must be taken to maintain the confidentiality and integrity of the information . This includes, but is not limited to employees, contractors and associates ensuring that Confidential Information is:
  - a) Stored with strong password protection, with devices and files is kept locked when not in use.
  - b) Not transported in see-through or other unsecured bags or cases, when in paper copy.
  - c) Not read in public areas when working remotely (e.g., in waiting rooms or on trains), and
  - d) Not left unattended or in a y place where it is at risk (e.g., in airports or conference centres)
- 7.5 Care must be taken to verify all postal and email addresses before any information is sent to them. Particular care must be taken when checking and verifying email addresses where auto-complete features may have inserted

incorrect email addresses.

- 7.6 Before being sent by email or recorded delivery, all sensitive or particularly Confidential Information should be encrypted.

## 8. **Personal email and cloud storage accounts**

- 8.1 Staff must not use personal email accounts or unauthorised cloud storage accounts for work purposes.
- 8.2 If large amounts of data need to be transferred employees should speak to Clayton John Ainger.

## 9. **Working from home**

- 9.1 Unless required for authorised business purposes, and then only in accordance with the subsequent paragraph, employees must not take information home with them.
- 9.2 Where information is permitted to be taken home, employees must ensure that appropriate technical and practice measures are in place within the home to maintain the continued security and confidentiality of that information. In particular, all Confidential Information and Personal Data must be:
- a) Kept in a secure and locked location, where it cannot be accessed by others (including family members and guests), and
  - b) Retained and disposed of in accordance with paragraph 5.4 above.
- 9.3 Employees must not store any Confidential Information on their home computers or other devices (e.g., laptops, PC's, or tablets).
- 9.4 For more information see the Company's Working from Home Policy.

## 10. **Transfer to third parties**

- 10.1 Third party service providers should only be engaged to process information where appropriate written agreement are in place to ensure that they offer appropriate data protection, confidentiality and information security protections and undertakings. Care must be taken to consider whether any such providers will be considered data processors for the purpose of the UK GDPR.
- 10.2 Employees involved in the process of setting up new arrangements or altering existing arrangements with third parties should speak to and consult with the DPO for more information and guidance.

## 11. International data transfers

11.1 There are restrictions on (onward) transfers of Personal Data to international organisations outside of the UK. Employees may not transfer Personal Data outside the UK (including to international organisations outside the UK). For more information speak with the DPO.

## 12. Computers and IT - Key Principles

- 12.1 All IT Systems and data are to be protected against unauthorised access.
- 12.2 All IT Systems and data are to be used only in compliance with relevant Company Policies.
- 12.3 All Personal Data must be used only in compliance with the Data Protection Legislation and the Company's Data Protection Policy.
- 12.4 All employees of the Company and any and all third parties authorised to use the IT Systems and data collected, held, and processed by the Company including, but not limited to, contractors and associates (collectively, "Users"), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.
- 12.5 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 2.4.
- 12.6 All data must be managed securely in compliance with all relevant parts of the Data Protection Legislation and all other applicable laws whether now or in the future in force.
- 12.7 All data must be classified appropriately (including, but not limited to, Personal Data, "special category" Personal Data (as described in Article 9 of the UK GDPR), and Confidential Information ). All data so classified must be handled appropriately in accordance with its classification.
- 12.8 All data, whether stored on IT Systems or in hardcopy format, shall be available only to those Users with a legitimate need for access.
- 12.9 All data, whether stored on IT Systems or in hardcopy format, shall be protected against unauthorised access and/or processing.
- 12.10 All data, whether stored on IT Systems or in hardcopy format, shall be protected against loss and/or corruption.
- 12.11 All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the IT Department or by such third party/parties as the IT Department may from time to time authorise.
- 12.12 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.
- 12.13 The responsibility for the security and integrity of data that is not stored on the

IT Systems lies with the Data Protection Officer, Clayton John Ainger who can be contacted by email at [clayton@castcommercialacumen.co.uk](mailto:clayton@castcommercialacumen.co.uk) or by mobile on 07495 818618.

- 12.14 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 Data Protection Officer.
- 12.15 All breaches of security pertaining to data that is not stored on the IT Systems shall be reported and subsequently investigated by the Data Protection Officer.
- 12.16 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 Data Protection Officer.
- 12.17 All Users must report any and all security concerns relating to data that is not stored on the IT Systems immediately to the Data Protection Officer.

### 13. Department Responsibilities

13.1 Clayton John Ainger, shall be responsible for the following:

- a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Company's security requirements.
- b) ensuring that IT security standards within the Company are effectively implemented and regularly reviewed, working in consultation with the Company's senior management and Data Protection Officer, as appropriate, and reporting the outcome of such reviews to the Company's senior management.
- c) ensuring that all Users are kept aware of the IT-related 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 Data Protection Legislation and the Computer Misuse Act 1990.

13.2 The Data Protection Officer, shall be responsible for the following:

- a) ensuring that all other data processing systems and methods are assessed and deemed suitable for compliance with the Company's security requirements.
- b) ensuring that data security standards within the Company are effectively implemented and regularly reviewed, working in consultation with the Company's senior management and Data Protection Officer, as appropriate, and reporting the outcome of such reviews to the Company's senior management.
- c) ensuring that all Users are kept aware of the non-IT-related 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 Data Protection Legislation.

13.3 The IT Staff shall be responsible for the following:

- a) assisting all Users in understanding and complying with the IT-related aspects of 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 Data Protection Officer.
- e) taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness.
- f) assisting the IT Manager in monitoring all IT security within the Company 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 at intervals no less than one week and that such backups are stored at a suitable location onsite.

13.4 The Data Protection Officer, shall be responsible for the following:

- a) assisting all Users in understanding and complying with the non-IT-related aspects of this Policy.
- b) providing all Users with appropriate support and training in data security matters.
- c) ensuring that all Users are granted levels of access to data that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements.
- d) receiving and handling reports concerning non-IT-related data security matters and taking appropriate action in response including, in the event that any reports relate to Personal Data, informing the Data Protection Officer.
- e) taking proactive action, where possible, to establish and implement security procedures and raise User awareness.

## 14. **Users' Responsibilities**

14.1 All Users must comply with all relevant parts of this Policy at all times when using the IT Systems and data.

14.2 All Users must use the IT Systems and data only within the bounds of UK law and must not use the IT Systems or data for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.

14.3 Users must immediately inform the IT Department and/or the Data Protection



Officer, of any and all security concerns relating to the IT Systems or data.

- 14.4 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.
- 14.5 Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the Company's disciplinary procedures.

## 15. **Software Security Measures**

- 15.1 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.
- 15.2 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 Data Protection Officer shall be informed immediately.
- 15.3 No Users may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the IT Manager. Any software belonging to Users must be approved by the IT Manager 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.
- 15.4 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 IT Manager. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

## 16. **Anti-Virus Security Measures**

- 16.1 Most 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.
- 16.2 All IT Systems protected by anti-virus software will be subject to a full system scan at least once a month.
- 16.3 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.
- 16.4 Users shall be permitted to transfer files using cloud storage systems only with the approval of the IT Manager. All files downloaded from any cloud storage

system must be scanned for viruses during the download process.

- 16.5 Any files being sent to third parties outside the Company, 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.
- 16.6 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 within 48 hours to limit disruption to the User.
- 16.7 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 Data Protection Officer.
- 16.8 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 the Company's disciplinary procedures.

## 17. **Hardware Security Measures**

- 17.1 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).
- 17.2 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.
- 17.3 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 IT Manager. 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 IT Manager.
- 17.4 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.
- 17.5 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company 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

or Company premises. 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.

- 17.6 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.

## 18. Organisational Security

- 18.1 All Users handling data (and in particular, Personal Data) will be appropriately trained to do so.
- 18.2 All Users handling data (and in particular, Personal Data) will be appropriately supervised.
- 18.3 All Users handling data (and in particular, Personal Data) shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to such data, whether in the workplace or otherwise.
- 18.4 Methods of collecting, holding, and processing data (and in particular, Personal Data) shall be regularly evaluated and reviewed.
- 18.5 All personal and non-Personal Data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy.
- 18.6 The performance of those Users handling Personal Data shall be regularly evaluated and reviewed.
- 18.7 All Users handling Personal Data will be bound to do so in accordance with the principles of the Data Protection Legislation and the applicable Company Policies by contract.
- 18.8 No data, personal or otherwise, may be shared informally and if a User requires access to any data, personal or otherwise, that they do not already have access to, such access should be formally requested in writing from Clayton John Ainger.
- 18.9 No data, personal or otherwise, may be transferred to any unauthorised User without the written authorisation of Clayton John Ainger.
- 18.10 All data must be handled with care at all times and should not be left unattended or on view to unauthorised Users or other parties at any time.

## 19. Access Security

- 19.1 Access privileges for all IT Systems and data shall be determined on the basis of Users' levels of authority within the Company and the requirements of their job roles. Users shall not be granted access to any IT Systems or data which are not reasonably required for the fulfilment of their job roles.
- 19.2 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.

- 19.3 All passwords must, where the software, computer, or device allows:
- a) be at least 15 characters long.
  - b) contain a combination of upper- and lower-case letters, numbers, and symbols.
  - c) be changed at least every 30 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.
- 19.4 Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone, including the IT Manager 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, where Personal Data could be accessed by an unauthorised individual, the Data Protection Officer.
- 19.5 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).
- 19.6 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 2 minutes of inactivity.
- 19.7 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company shall be set to lock, sleep, or similar, after 2 minutes of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake, or similar.
- 19.8 Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the IT Manager. 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 IT Manager and, where such access renders Personal Data accessible by the outside party, the Data Protection Officer.
- 19.9 Users may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the Company network 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 the Company 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 the Company 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.

## 20. **Data Storage Security**

- 20.1 All data stored in electronic form, and in particular Personal Data, should be stored securely using passwords and where possible data encryption.
- 20.2 All data stored in hardcopy format or electronically on removable physical media, and in particular Personal Data, should be stored securely in a locked box, drawer, cabinet, or similar.
- 20.3 No Personal Data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise.
- 20.4 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 the Company and that User has agreed to comply fully with the Company's Data Protection Policy and the Data Protection Legislation.

## 21. **Data Protection**

- 21.1 All Personal Data collected, held, and processed by the Company will be collected, held, and processed strictly in accordance with the principles of the Data Protection Legislation, the provisions of the Data Protection Legislation and the Company's Data Protection Policy.
- 21.2 All Users handling data for and on behalf of the Company shall be subject to, and must comply with, the provisions of the Company's Data Protection Policy at all times. In particular, the following shall apply:
  - a) All emails containing Personal Data and/or other data covered by this Policy, where possible, be encrypted.
  - b) All emails containing Personal Data and/or other data covered by this Policy must be marked "confidential".
  - c) Personal Data and/or other data covered by this Policy may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances.
  - d) Personal Data and/or other data covered by this Policy may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
  - e) Personal Data and/or other data covered by this Policy 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.
  - f) All Personal Data and/or other data covered by this Policy to be transferred physically, including that on removable electronic media, shall be transferred in a suitable container marked "confidential".

- g) Where any Personal Data and/or other data covered by this Policy 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.

21.3 Any questions relating to data protection should be referred to [the Data Protection Officer.

## 22. Deletion and Disposal of Data

22.1 When any data, and in particular Personal Data, is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it must be securely deleted and/or disposed of.

22.2 For further information on the deletion and disposal of Personal Data, please refer to the Company's Data Retention Policy.

## 23. Internet and Email Use

23.1 All Users shall be subject to, and must comply with, the provisions of the Company's Communications, Email, Internet Policy, and Social Media Policy when using the IT Systems.

23.2 Where provisions in this Policy require any additional steps to be taken to ensure security when using the internet or email over and above the requirements imposed by the Communications, Email, Internet Policy and Social Media Policy, Users must take such steps as required.

## 24. Reporting Security Breaches

24.1 Subject to paragraph 24.3, all concerns, questions, suspected breaches, or known breaches that relate to the IT Systems shall be referred immediately to Clayton John Ainger.

24.2 Subject to paragraph 14.3, all concerns, questions, suspected breaches, or known breaches that relate to other data covered by this Policy shall be referred immediately to Clayton John Ainger.

24.3 All concerns, questions, suspected breaches, or known breaches that involve Personal Data shall be referred immediately to the Data Protection Officer who shall handle the matter in accordance with the Company's Data Protection Policy.

24.4 Upon receiving a question or notification of a breach, the individual or department responsible 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 deemed necessary to respond to the issue.

24.5 Under no circumstances should a User attempt to resolve a security breach on their own without first consulting the relevant individual or department (or the Data Protection Officer, as appropriate).

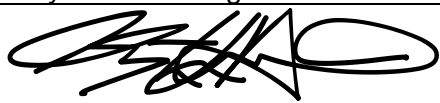
24.6 All security breaches, howsoever remedied, shall be fully documented.

**25. Consequences of non-compliance**

- 25.1 The Company takes compliance with this policy very seriously and failure to comply with this policy puts Users and the Company alike at significant risk.
- 25.2 Due to the importance of this policy, failure to comply with any of its procedures and requirements may result in disciplinary action, dismissal, or cancellation of a contract for contractor and associates.
- 25.3 If you have any questions or concerns about anything in this policy, please contact the DPO at [clayton@castcommercialacumen.co.uk](mailto:clayton@castcommercialacumen.co.uk)

**26. Policy Review and Implementation**

- 26.1 The Company shall review this Policy not less than two years and otherwise as required in order to ensure that it remains up-to-date and fit for purpose.
- 26.2 This Policy will be updated as necessary to reflect current best practice, official guidance, and in line with current legislation.
- 26.3 This Policy shall be deemed effective as of 13th April 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

<b>Document title:</b>	Information and Data Security Policy
<b>Document status:</b>	Final
<b>Version number:</b>	1.0
<b>Date:</b>	April 2023
<b>Review date:</b>	April 2025
<b>Owner:</b>	Managing Director
<b>Approved by:</b>	Clayton John Ainger
<b>Signature:</b>	

**This Information and Data Security Policy is not contractual and may be varied by Cast Commercial Acumen Limited at any time.**