

CAST COMMERCIAL ACUMEN LIMITED

Bringing Own Devices to Work (BYOD) Policy

1. Introduction

This policy applies to employees who work remotely, contractors and associates working with, and/or on behalf of the Company who bring their computers and/or other electronic devices, such as smartphones, mobile phones and tablets into work. This Policy on Bringing Own Devices to Work (BYOD) is intended to protect the security and integrity of any personal data and the Company's technology infrastructure. It should be read in conjunction with the Company's Communications, Email, Internet Policy and Social Media Policy.

With the prior agreement of Clayton John Ainger, all employees, contractors, and associates are permitted to use their own devices for work-related purposes. However, employees, contractors and associates must agree to the terms and conditions set down in this policy to be able to connect their devices to the company network and use their own devices for work-related purposes.

2. Acceptable Use

The employee, contractor or associate is expected to always use his or her devices in an ethical manner in accordance with the Company's Communications, Email, Internet Policy, Social Media Policy and Data Protection Policy.

The company defines acceptable use of own devices as:

- activities that directly or indirectly support the business of the Company.
- reasonable and limited personal communication or recreation, such as reading or game playing.

Devices may not be used at any time to:

- Store or transmit illicit materials.
- Store or transmit proprietary information belonging to another company.
- Harass others.
- Engage in outside business activities whilst working with the Company.

Employees may use their mobile device to access the following Company-owned resources: email, calendars, contacts, presentations, spreadsheets, videos, and documents.

Employees should be aware that any personal device used at work may be subject to discovery in litigation and may be used as evidence in any action against the Company (see also 5.3 below).

3. **Data Protection**

Cast Commercial Acumen Limited is the data controller in respect of work-related personal data that is held on personal devices. Clayton John Ainger is the Company's data protection officer and is responsible for the implementation of this policy.

Data Protection law in the UK requires the Company to process personal data in accordance with the six data protection principles. The Company must:

- Process personal data fairly, lawfully, and transparently
- Obtain and process data only for one or more specified and lawful purposes.
- Ensure that data is adequate, relevant, and limited to what is necessary.
- Ensure that data is accurate and kept up to date.
- Not keep data longer than necessary.
- Take appropriate technical and organisational measures against accidental loss or destruction of, or damage to, personal data.

4. **Special Category Data**

"Special category data" is information about an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or philosophical beliefs
- trade union membership
- physical or mental health or condition
- sex life or sexual orientation.

Employees, contractors, and associates must not process special category data on a personal device that relates to the Company, its employees, clients, or business contacts. If any special category data is stored on a device, it must be permanently deleted from the device.

5. **Obligations in respect of BYOD**

5.1 Security

- To prevent unauthorized access, devices must be password protected using a strong password.
- Any device used must lock itself with a password or PIN if it is idle for five minutes.
- Any device used must be capable of locking automatically if an incorrect password is entered after several attempts.
- Employees must ensure that, if they transfer data, they do so via an encrypted channel e.g., a VPN.
- Employees must not download unverified apps that may present a threat to the security of the information held on their devices.
- Employees should not use unsecured networks.

- The loss of a device used for work-related activities must be reported at the earliest opportunity to Clayton John Ainger.
- Employees must report data breaches to Clayton John Ainger immediately.

5.2 Devices and Support

- Devices must be presented to Clayton John Ainger for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before employees can access the network.

5.3 Cooperation with subject access requests

- Any individual whose personal data is held by the Company has the right to make a subject access request. Consequently, the Company may have to access your device to retrieve any data that is held on it about the individual. You must allow the Company to access the device and carry out a search for information about an individual that may be held on the device.

5.4 Retention of Personal Data

- Employees, contractors, and associates must not keep personal data for longer than necessary for the purpose for which it is being used, unless there is a requirement to retain it for longer in order to comply with a legal obligation.

5.5 Deletion of Personal Data

- Employees, contractors, and associates must ensure that, if they delete information from a device, the information must be permanently deleted rather than left in the device's waste management system.
- If removable media, e.g., a USB drive or CD, is used to transfer personal data, employees must ensure that the personal data is deleted after the transfer is complete.

5.6 End of Employment, Contract or Engagement with the Company

- Prior to the last day of employment or contract with the Company, all employees, contractors, or associates must delete work-related personal data on his/her own device.

5.7 Third-Party Use of Devices

- Employees, contractors, and associates must ensure that, in the event of friends or family using their devices, they are not able to access any work-related personal information by, for instance, password-protecting the information.

6. Monitoring

As part of its obligations under the law, the Company will monitor data protection compliance in general and compliance with this policy in particular. The monitoring is in the Company’s legitimate interests to ensure compliance with this policy and to ensure that the Company is complying with its obligations under the UK’s data protection legislation.

Before any monitoring is undertaken, the Company will identify the specific purpose of the monitoring.

Monitoring will seek to ensure that the employee, contractor, or associates’ devices are compliant with this policy.

6 Non-Compliance

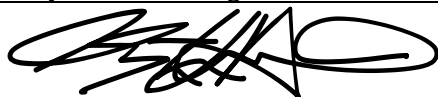
Any employee, contractor or associate found to be breaching this policy will be asked to rectify the situation within 48 hours. Non-compliance by a contractor or associate could result in their contract / engagement with the Company being terminated. Non-compliance by an employee will be treated in accordance with the Company’s disciplinary procedure.

8 Review and Training

The Company will provide data protection training to all employees on a regular basis. This BYOD policy will be reviewed on an annual basis.

7. Implementation of Policy

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.

Document title:	Bring Your Own Devices to Work Policy (BYOD)
Document status:	Final
Version number:	1.0
Date:	April 2023
Review date:	April 2025
Owner:	Managing Director
Approved by:	Clayton John Ainger
Signature:	

This Bring Your Own Devices to Work Policy is not contractual and may be varied by Cast Commercial Acumen Limited at any time.