

BRING YOUR OWN DEVICE (BYOD) POLICY

1. INTRODUCTION

- 1.1 This policy contains the bring your own device policy Winder Research and Development Ltd (the Company).
- 1.2 The Company reserves the right to amend, replace or remove the contents of this policy from time to time, in its absolute discretion. Any amendments or revisions will be notified to staff by email and subsequently incorporated into future editions.
- 1.3 Staff members are required to familiarise themselves with the contents of this policy and comply with it at all times.
- 1.4 This policy applies when staff are using their own devices on or off the Company's premises.
- 1.5 This policy should be read in conjunction with the Company's IT, communications and social media policy and Data protection policy.

2. PERMITTED DEVICES

- 2.1 All Staff members are permitted to use their own personal electronic devices, including laptops, mobile phones and tablets, in the workplace for work related purposes in accordance with this policy.

3. ACCEPTABLE USE

- 3.1 All personal electronic devices must be used responsibly at all times and in accordance with the Company's Data protection policy and the general rules regarding the use of IT equipment, as set out in the Company's IT, communications and social media policy.
- 3.2 Devices that are not approved in accordance with this policy must not be used to connect to the Company's network.
- 3.3 Staff members must disable the use of camera and/or video functionalities whilst they are using their personal devices on the Company's premises.
- 3.4 The Company may monitor the use of its IT systems even where such use occurs through personal devices authorised for work related activities in accordance with this policy. Any such monitoring will be carried out in accordance with the Company's IT, communications and social media policy and its Data protection policy.

4. SECURITY

- 4.1 All personal electronic devices must be password protected in accordance with the password policy set out in the Company's IT, communications and social media policy.
- 4.2 If left idle for five minutes, devices must be set to lock themselves with a password or PIN to prevent unauthorised access.
- 4.3 Staff members must ensure that personal devices used for work activities are updated with the latest software and that encryption and anti-virus protection is activated (where relevant).

- 4.4 To enable devices to be wiped remotely in event of loss, theft or damage, relevant software to track and/or wipe devices must be installed and configured (where appropriate).
- 4.5 If a device that has been authorised and used for work related purposes in accordance with this policy is lost, stolen or damaged, staff members must report this to Phil Winder as soon as they become aware of the loss, theft or damage.
- 4.6 The Company assumes no liability for any losses incurred as a result of the loss, theft or damage to a staff member's personal device.

5. DATA PROTECTION

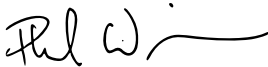
- 5.1 All staff members must comply with the Company's Data protection policy at all times.
- 5.2 Staff members must not store any personal data obtained or processed during the course of their work activities on their personal devices.
- 5.3 Any personal data that is processed using staff members' personal devices must be dealt with and subsequently deleted in accordance with the Company's Data protection policy.
- 5.4 In the event that the Company receives a data subject access request, staff members may be required to provide the Company with access to personal devices that have been used for work activities in order to retrieve and/or review any relevant personal data about the individual who has made the request. Staff members must cooperate with the Company and carry out reasonable searches for such information.

6. BREACH OF THIS POLICY

- 6.1 All staff members (including employees, casual workers, officers and agency workers) must comply with this policy. Any breach of this policy will be taken extremely seriously and, in the case of employees, may lead to disciplinary action up to and including dismissal.

7. END OF EMPLOYMENT OR HIRE

- 7.1 Before leaving the Company, staff members must ensure that all data and information relating to the Company's activities is deleted from their personal devices.

Signed: 

Phil Winder

CEO

8 August 2022