IT, COMMUNICATIONS AND SOCIAL MEDIA POLICY

1. This Policy contains the IT, communications and social media policies of Winder Research and Development Ltd (the Company).

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.

3. Staff members are required to familiarise themselves with the contents of this policy and comply with it at all times.

4. All staff have a responsibility to ensure the security of IT equipment allocated to or used by them. Staff must ensure that they use the Company's IT equipment in accordance with this policy.

5. The Company's general rules regarding the use of IT equipment are as follows:

    A. all IT equipment must be password, PIN or touch-ID protected as appropriate;

    B. staff must never use default passwords or PINs and must keep passwords and PINs confidential at all times, changing them regularly;

    C. staff must only ever log in to the Company's IT systems using their own username and password and must not share their log on details with other staff;

    D. staff must lock their computers when away from their desks, and any other devices when not in use;

    E. staff must log out and shut down computers at the end of each working day;

    F. staff must not delete, destroy or modify any software or hardware, unless authorised in advance or, if their role includes IT responsibilities, in the proper performance of their duties;

    G. staff must not download or install any software on Company computers or devices without prior authorisation from Phil Winder;

    H. staff must not use or attach any external devices to the Company's IT equipment, including mobile phones, tablet computers or USB drives;

    I. staff should be mindful of opening unknown emails as they may contain viruses; if in doubt, report a suspicious email to Phil Winder: do not open it, click on any links or open any attachments;

    J. staff must not access any material using Company IT equipment that would be considered criminal, abusive, obscene, pornographic, racist, discriminatory, or defamatory;

    K. staff must not access any information which is confidential to the Company or its clients, or to other staff members, except in the proper course of their duties and where authorised to do so;

L. staff may access the internet for personal use, including access to web-based email systems such as Hotmail or Gmail during their break periods. Such access must be minimal, otherwise the Company may take appropriate action to restrict such access or take disciplinary action.

6. Staff are required to adopt a professional standard in their written communication over email, particularly when communicating with third parties. Staff are reminded that all emails are capable of being disclosed as part of legal proceedings.

7. Staff must not use the Company's email system for private emails or to engage in non-work-related communications. Staff must not use their personal email accounts to conduct work related activities.

8. The Company may block or restrict access to certain websites at its discretion.

9. Any breach of IT security, misuse or excessive personal use of the Company's IT equipment, telephone or e-mail system or inappropriate internet use will be treated as a serious matter and in the case of employees will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

10. The Company may provide remote access to the Company network to allow for flexibility in working. The same security principles will apply in such circumstances. Additionally, staff members must be careful about the location they access the network from, and the equipment they use to do so to ensure the Company's information and systems are secure.

11. The Company may monitor telephone, e-mail, voicemail, internet and other communications for business reasons and to carry out the Company's legal obligations. The use of the Company's IT systems may be continually monitored by automated software or otherwise. The Company reserves the right to retrieve email contents or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of alleged wrongdoing and to comply with any legal obligation.

12. The occasional use of social media during working hours is permitted provided it does not interfere with work and complies with Company policy.

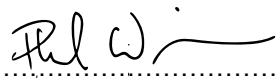
13. Staff must avoid using social media in any way that could damage the Company's business interests or reputation. Staff must not use social media in any way that defames or disparages the Company, other staff members or clients.

14. Staff members must not use social media to harass, bully or unlawfully discriminate against anyone or to make false or misleading statements.

15. Staff must not use social media to comment upon sensitive Company topics such as financial performance or do anything that might breach duties of confidentiality owed to the Company.

16. Staff must not express opinions or use the Company's logo or branding on social media on behalf of the Company without prior authorisation and must make clear on any personal social media accounts that any opinions expressed are their own and cannot be construed as being those of the Company.

17. If staff are aware of any abuse of this social media policy, it should be reported to Phil Winder as soon as possible. Any breach of this policy may result in disciplinary action up to and including dismissal.

Signed: 

Phil Winder

CEO

8 August 2022