



IT and Communications Systems Policy

Company Policy No: 8

Company: Direct Healthcare 24 t/a Little Steps Staffing Ltd

Issue No: 2

Revision Date: April 2026

Review Date: April 2027

IT and Communications Systems Policy

Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.

This policy covers all employees, officers, consultants, contractors, casual workers, agency workers and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can damage the business and our reputation. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

The following standards apply to your access and disclosure of electronic material created, sent, received or stored either via the Internet or our internal networks by employees. Electronic material includes e-mails, or any material that can be downloaded via the Internet or sent across our computer network:

- 1) Your computer systems are maintained solely for conducting our business. The use of the Internet and e-mail for any other purpose may be subject to action under our disciplinary procedure.
- 2) You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision.
- 3) You should use passwords on all IT equipment, particularly items that you take out of the office. You must keep your passwords confidential and change them regularly. You must not use another person's username and password or make available or allow anyone else to log on using your username and password unless authorised by Human Resources to do so. On the termination of employment (for any reason) you must provide details of your passwords on request, and return any equipment, key fobs or cards.
- 4) If you have been issued with a laptop, tablet computer, BlackBerry, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft.
- 5) You should be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.
- 6) You should not delete, destroy or modify existing systems, programs, information or data (except as authorised by Human Resources in the proper performance of your duties).

- 7) You must not download or install software from external sources without authorisation from the IT Director. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.
- 8) You must not attach any device or equipment to our systems without authorisation from the IT Director. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way.
- 9) You must inform the IT Helpdesk immediately if you suspect your computer may have a virus.
- 10) You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised by Human Resources in the proper performance of your duties.
- 11) Computers, networks and e-mail systems are our property. All copies of messages created, sent, received or stored on our systems shall remain our property. Messages are not the private property of employees and as such there should be no expectation of privacy in any circumstances. If you use our email address for communication that is not business related you waive any privacy or any other rights that you have in relation to such communications and consent to their being read, monitored, recorded and otherwise intercepted by us.
- 12) We reserve the right to access and monitor all messages created, sent, received or stored on our systems. The contents of e-mail messages may be disclosed internally and to third parties without further permission and at our discretion. You must remember that even when an e-mail message is deleted it is still possible for the message to be retrieved and read. The use of passwords does not assure confidentiality and the existence of a password does not restrict our right to access e-mail messages.
- 13) Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter and you must adopt a professional tone and observe appropriate etiquette. Messages should be concise and directed only to relevant individuals.
- 14) E-mails, text messages and the Internet should not be used to create, send, receive or store any material which is discriminatory, offensive, obscene, contains images depicting sexual activity or bodily parts in a lewd manner or which are pornographic, disruptive or infringe copyright. Our policies with regard to discrimination or harassment apply fully to the Internet and e-mails and text messages. The same laws apply to e-mail as to any other written documents and therefore any comments that could be regarded as defamatory, inaccurate or misleading should be avoided. Use of our computers, telephone lines, telephone systems, internet connection or any other system or software or equipment owned or controlled by, leased or rented to us to access Internet sites or download or receive email or other electronic images or media that contains pornography or other obscene or illegal contents shall constitute gross misconduct that can lead to your dismissal without notice.
- 15) Notwithstanding our right to retrieve and read any e-mail messages, you should treat e-mails as confidential and only the intended recipient must open them. Only disclose information or

messages obtained from e-mails to recipients authorised to have such information.

- 16) All e-mails and downloads can contain viruses. Therefore, all downloads and e-mail messages must be virus-checked before opening. It is also a term of your contract of employment that you are not allowed to load software on to your computer without our permission
- 17) You should not access any webpage or download any image or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, viewing a webpage will be a breach of this policy if:
 - a. any person (whether intended to view the webpage or not) might be offended by its contents; or
 - b. the fact that our software has accessed the webpage or file might be a source of embarrassment if made public.