



E-mail, Telephone, Internet and Computer Facilities Policy

September 2022

1st Homecare Solutions Ltd.
5a Ridgeway Court
Grovebury Road
Leighton Buzzard
Bedfordshire
LU7 4SF

Tel: 01525 376677

1st Homecare (Oxford) Ltd
Ground Floor,
8 Isis Business Centre
Pony Road
Oxford
OX4 2RD

Tel: 01865 744174

1st Homecare Kings Langley
Unit 15 Sunderland Estate
Church Lane
Kings Langley
WD4 8JU

Tel: 01923 269877

1 OVERALL PURPOSE OF POLICY

Set out below is 1st Homecare's policy for the use of telephone (landline and mobile) and computer facilities (fixed, laptop and I-pad) including use of e-mail and the internet ("the facilities") by employees working for 1st Homecare.

2 MONITORING OF USE

The facilities are made available to employees to enable them to carry out the business of 1st Homecare. As such, 1st Homecare has the right to monitor use of the facilities that are made available to staff and to monitor, intercept and/or record any communications made by using the facilities. This is to ensure compliance with this Policy, with all 1st Homecare's policies and procedures, and with regulations and standards that regulate the business of 1st Homecare or for any other purpose authorised under the Investigatory Powers (Interception by Businesses etc for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356) (which replace (and largely mirror) the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)).

The Investigatory Powers (Interception by Businesses etc for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356) provide that organisations and public bodies may lawfully intercept communications being sent via their telecommunications systems for certain legitimate business activities. These activities include establishing whether or not staff using the organisation's telecommunications system are achieving the standards required by the company in the course of their duties.

By using the facilities, employees consent voluntarily and knowingly to their use being monitored, and also acknowledge the right of 1st Homecare to conduct such monitoring.

3 CONFIDENTIALITY AND DATA PROTECTION

A high degree of caution must be exercised when using the email and internet to ensure that confidential information is not transmitted to any person who does not have the right to access it. Care must be used in addressing data or messages to make sure that they are not sent to the wrong individual or company. In particular, employees should exercise care in using e-mail distribution lists to make sure that all addressees are appropriate recipients of the information. The Company's Confidentiality Policy should be referred to for the Company's overall policy on confidential information. The Company's Data Protection Policy should also be referred to.

4 CONTENT OF EMAIL OR MOBILE MESSAGES

It is important that staff take care to ensure that all messages are courteous, professional and business-like. On mobile messages, proper language should be used, numbers should not be substituted for words for example. Messages should also not contain any material which would reflect badly on 1st Homecare's reputation. Messages must not contain derogatory remarks about another person, as this may constitute libel. If any staff member receives a message containing material that is offensive or inappropriate, then they must delete it immediately. Under no circumstances should such a message be forwarded internally or externally.

5 USAGE

The facilities may be used, within reason, for personal communications and to browse external web sites or go to social networking sites for personal use provided this is done outside office hours. If there is evidence that this privilege is being abused then the privilege may be withdrawn. The content of personal e-mails and any use of social networking sites must comply with the restrictions set out in this Policy and in the Company's Use of Social Media Policy, the Confidentiality Policy, the Equality and Diversity, Bullying and Harassment Policy, and the Data Protection Policy.

The following uses of the facilities are expressly prohibited:

- Viewing internet sites containing pornographic, obscene, abusive, slanderous or otherwise offensive material or downloading/forwarding such material
- Communications that are in violation of Company policy - including, but not limited to, the transmission of defamatory, obscene, offensive or harassing messages, or messages that disclose information without appropriate authorisation
- Duplicating copyrighted or licensed software or other information without the appropriate authorisation
- Installing or downloading any software or hardware without the specific approval of the CEO/Registered Manager or other person delegated by him/her to give such approval
- Forwarding or otherwise perpetuating "chain-letter" type e-mail within or outside the Company
- Removal of any hardware or software without prior approval from the CEO /Registered Manager

6 TELEPHONE USAGE

Landline phones

Company landlines should be kept for work use save for exceptional circumstances.

As noted above, the Investigatory Powers (Interception by Businesses etc for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356) provide that organisations and public bodies may lawfully intercept communications being sent via their telecommunications systems for certain legitimate business activities. These activities include establishing whether or not staff are achieving the standards required by the Company. All telephone calls on the Company's landline system are recorded for training and monitoring purposes and this is announced to all callers via a pre-recorded message.

Mobile phones

1st Homecare uses a care management mobile app, Access Care Planning, and for administrative reasons and to ensure the security and confidentiality of data accessed by staff, issues staff with a Company owned mobile phone.

Staff receive client visit rotas on their Company owned mobile phone to better ensure security and confidentiality of client data.

Staff are required to enter into an Agreement with 1st Homecare recording the terms and conditions of use of their Company mobile phone.

As a benefit of having the use of a Company owned mobile phones, staff are provided with unlimited calls and texts, and may use it for personal calls and texts except for premium lines and overseas calls, which are blocked.

Staff may access apps on their Company owned mobile phone but some apps are blocked by 1st Homecare at management discretion.

Staff are responsible for keeping secure the password for their mobile phone and must not disclose it to any person whatsoever. The password should not be stored in a form where it might be accessed by any other person. Security settings are set up by 1st Homecare on phones to ensure security of information and must not be changed.

7 HOUSEKEEPING

Large quantities of e-mails or downloaded files or attachments should not be stored as the retention of such data utilises large amounts of storage space on both network servers and computers and may adversely affect system performance. Staff should delete any e-mail messages sent or received that no longer require action or are no longer relevant. Any emails containing information that need to be retained for record-keeping purposes should be stored in the appropriate folder on Dropbox.

8 SECURITY

Staff should let a manager know immediately if they receive any suspect documents, e-mail messages or computer virus alerts. Staff must **not open attachments to any email message that is from an address that they do not recognise**. These should not be forwarded to any other internal or external user. Any files or software downloaded from the Internet or brought from home must be virus-checked before use.

9 PASSWORDS

Passwords should be kept secure and be changed regularly. To protect passwords, staff should not login to the facilities in the presence of others where the login details can be seen, and passwords should not be saved onto the computer. Confidential information should never be left open on the screen when equipment is unattended. Reference should be made to the Company's Confidentiality Policy in this regard.

10 NON-COMPLIANCE

Failure to comply with the Policy may lead to disciplinary action up to and including dismissal (for serious breaches) in accordance with 1st Homecare's Discipline and Grievance Procedure.

11 GENERAL

This Policy may be amended or altered at any time. Employees will be notified of such changes.

E-mail, Telephone, Internet and Computer Facilities Policy

CHANGE HISTORY

Issue	Date	Description of Change and Reason
1	November 2012	First Issue
2	December 2013	Second Issue
3	November 2014	Third Issue
4	October 2016	Fourth Issue – no changes
5	February 2017	Fifth Issue – changes to make applicable to both businesses
6	October 2018	Sixth Issue – change to address of Company
7	January 2020	Seventh Issue – change to the legislation on interception and monitoring of communications, inclusion of KL office address
8	September 2022	Eighth Issue – grammatical changes, main change is to update the Policy to cover issuance of Company owned mobile phones and permitted use of these.

DOCUMENT CONTROL

Name of document	E-mail, Telephone, Internet and Computer Facilities Policy
Status	Issued
Issue	8
Issue date	September 2022
Maintainer	1HC
Owner	1HC
File name	1HC E-mail, Telephone, Internet and Computer Facilities Policy
File location	New policies/HR
Review date	September 2024