

# LAND RECOVERY

## IT CODE OF CONDUCT POLICY

### 1. INTRODUCTION

This document provides rules and guidance for the correct use of information technology and communications facilities within Land Recovery Ltd and Land Recovery Rail Ltd (from herein all references to Land Recovery Ltd will imply the same to Land Recovery Rail Ltd).

The policy covers the use of

- Company supplied computer hardware including but not limited to desktop computers, laptops, tablets portable devices, smart phones
- Software
- Telecommunications
- Email
- Internet technologies
- Accessing company data and systems through the use of personal computer hardware including but not limited to desktop computers, laptops, tablets, portable devices and smartphones

It applies to all employees regardless of job, task or function.

Email communications facilities are provided by Land Recovery Ltd and made available to users for the purposes of the business. A certain amount of limited and responsible personal use by users is also permitted. All use of our communications facilities is governed by the terms of this policy, and if our rules and procedures are not adhered to, then use of our facilities may be curtailed or withdrawn and disciplinary action may follow. Any breach of this policy may lead to disciplinary action being taken against you and serious breaches may lead to summary dismissal.

- 1.1 At Land Recovery Ltd communication plays an essential role in the conduct of our business. How you communicate with people not only reflects on you as an individual but also on us as an organisation. We value your ability to communicate with colleagues, clients/customers and business contacts, and we invest substantially in information technology and communications systems which enable you to work more efficiently. We trust you to use them responsibly.
- 1.2 This policy applies to all individuals working for Land Recovery Ltd who use our communications facilities, whether directors / departmental heads / partners / consultants, full-time, part-time or fixed-term employees, trainees, contract staff, temporary staff, agency or home workers.
- 1.3 Whilst the IT Policy is primarily focused on the use of applications software, email and internet facilities, the general principles underlying all parts of this policy also apply to telephone communications, copiers and scanners. Note that some elements of personal use of Land Recovery Ltd communications facilities are specifically addressed at items 3.3, 4.3 to 4.5, 9.4 and 9.5, and 10.5. Please read this policy carefully.

### 2. GENERAL PRINCIPLES

- 2.1 You must use Land Recovery Ltd information technology and communications facilities sensibly, professionally, lawfully, and consistently with your duties, with respect for your colleagues and others in accordance with this policy and in accordance with any other Land Recovery Ltd rules and procedures.
- 2.2 All information relating to our clients/customers and our business operations is confidential. You must treat our paper-based and electronic information with the utmost care.

This document is uncontrolled when printed, version control must be assured before use.

# LAND RECOVERY

- 2.3 Many aspects of communication are protected by intellectual property rights which are infringed by Copying; Downloading, uploading, posting, copying, possessing, processing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.
- 2.4 Particular care must be taken when using email, company blog or internal message boards as a means of communication because all expressions of fact, intention and opinion in an email may bind you and/or Land Recovery Ltd and can be produced in court in the same way as other kinds of written statements.
- 2.5 The advantage of the internet and email is that they are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. All messages sent on email systems or via the internet should demonstrate the same professionalism as that which would be taken when writing a letter or a fax. You must not use these media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any discriminatory (on the grounds of a person's sex, race, disability, age, sexual orientation, religion or belief), defamatory, or other unlawful material (for example, any material that is designed to be, or could be construed as, bullying or harassment by the recipient). If you are in doubt about a course of action, take advice from your line manager/departmental head.
- 2.6 All information residing on the Land Recovery Ltd computer systems remains the property of the business at all times.
- 2.7 All hardware / software used by employee's remains the property of the Land Recovery Ltd at all times.
- 2.8 The computer hardware has been set up to run only the software installed by the IT Department or its third party representatives. All the licensed programs and hardware which have been installed have been tested and verified as to their suitability.
- 2.9 You are expressly forbidden to:
- 2.9.1 Install or load any software or program brought from home / previous employer / supplier or any other source without the express permission from the IT Department.
- 2.9.2 Use your own personal PC or a third parties PC linked to the company network without the express permission of the IT Department.
- 2.9.3 Make copies of licensed business software with the exception of any software made available to staff as a benefit of the Microsoft CSP Agreement provided it has been paid for and downloaded directly from Microsoft. Staff taking advantage of this benefit must ensure they understand the license agreement and usage for which the software is intended.
- 2.9.4 Transfer data from a business computer to a private computer without gaining express permission from your line manager or the IT Department. The term 'Transfer' includes sending via email, copying data via memory device or media or forwarding via any form of file transfer.
- 2.9.5 Alter, re-configure or remove business software or peripheral devices residing on or attached to a personal computer.
- 2.9.6 Alter, move, re-configure, non-portable hardware from the business (e.g. printers, terminals).

Exemptions are made for IT staff who may be required to carry out the above activities as a necessary part of their function.

## 2.11 Company Supplied Equipment

### 2.11.1 Laptop Computers

This document is uncontrolled when printed, version control must be assured before use.

# LAND RECOVERY

- (a) Staff provided with a laptop computer may use the equipment for work related purposes. The equipment must not be loaned or delegated to other family members or non- Land Recovery Ltd employees.
- (b) Laptop computers should not be left unsecured in open office areas or unlocked offices overnight. If laptops are to be left in company offices, they should be secured in a lockable desk or cabinet.
- (c) Laptop computers should not be left in vehicles overnight even if secured in the boot. Laptop computers should be taken into the home/hotel and secured in a safe if possible. In addition, laptop computers should not be left in vehicles for long periods if unattended during daytime e.g. whilst attending meetings or parking.

## 2.11.2 Tablet computers

- (a) Staff provided with a tablet computer may use the equipment for work related purposes. The equipment must not be loaned or delegated to other family members or non- Land Recovery Ltd employees.
- (b) Tablet computers should not be left unsecured in open office areas or unlocked offices overnight. If tablets are to be left in company offices, they should be secured in a lockable desk or cabinet.
- (c) Tablet computers should not be left in vehicles overnight even if secured in the boot. Tablet computers should be taken into the home/hotel and secured in a safe if possible. In addition, tablet computers should not be left in vehicles for long periods if unattended during daytime e.g. whilst attending meetings or parking.
- (d) Tablet computers should be secured with PIN code and/or secure usernames and passwords.
- (e) Where possible tablet computers should be enabled for remote tracking and wipe in the event of loss or theft.

## 2.11.3 Smartphones

- (a) Staff provided with a Smartphone may use the equipment for work related purposes. The nature of Smartphones allows for an element of personal use in order to download content and personalise devices. The equipment must not be loaned or delegated to other family members or non- Land Recovery Ltd employees.
- (b) Smartphones should not be left unsecured in open office areas or unlocked offices.
- (c) Smartphones should not be left in vehicles even if secured in the boot. Smartphones should be carried with the user and if not in use, taken into the home/hotel and stored securely.
- (d) Smartphones should be secured with PIN code and/or secure usernames and passwords and may be enforced by mobile device management software.
- (e) Where possible Smartphones should be enabled for remote tracking and wipe in the event of loss or theft.

## 2.11.4 Protection of company data

The company reserves the right to protect data stored on company supplied equipment. In the event of a device being stolen or lost the company will perform a remote wipe of the device. In the case of tablets and smartphones, this will reset the device to factory default settings. Any personal information stored on the device WILL be lost. The company does not back up personal applications or data, this is the responsibility of the user.

## 2.11.5 Inappropriate use of company supplied equipment

The company reserves the right to seize, for further investigation; any computer supplied equipment that it believes may have been used inappropriately.

## 2.12 Use of Personal Equipment

This document is uncontrolled when printed, version control must be assured before use.

# LAND RECOVERY

The company recognises that some staff may wish to use their own personal equipment to access company data and systems. The company will allow this use with the following stipulations.

- 2.12.1 Equipment is defined specifically as tablet computers and smartphones, connected via 3G/4G/WI-Fi access. Staff are not permitted to use their own PCs, Apple Macs, laptops connected to the company network, but can use these devices to access email via <https://office.com>
- 2.12.2 Access must be requested through an IT Service Desk User Amendment request and will not be granted without appropriate authorisation. Staff requesting access are also indicating their acceptance of this policy.
- 2.12.3 Access will be restricted to email only. File shares and applications will not be permitted.
- 2.12.4 Data attached to emails must not be stored locally on personal equipment.
- 2.12.5 Land Recovery Ltd IT Department will NOT support the configuration of staff supplied equipment.
- 2.12.6 Land Recovery Ltd is NOT responsible for any network charges incurred by staff in relation to their access of company data and systems from their own equipment. The company recommends that staff configure their devices to only retrieve the data they need.
- 2.12.7 Device must be secured with PIN or username/password and may be enforced via mobile device management software.
- 2.12.8 Staff must notify IT Service Desk as soon as possible in the event of their equipment being lost or stolen.
- 2.12.9 The company reserves the right to wipe data from an individual's equipment. This process will reset the device back to factory default.
- 2.12.10 The company is not responsible for backing up or the loss of any personal data, including but not restricted to applications, photos, videos, music, SMS messages etc.

## 3. USE OF ELECTRONIC MAIL

### 3.1 General

- 3.1.1 The default email template contains the appropriate disclaimer notice which is attached automatically to all externally sent email addresses.
- 3.1.2 Do not amend any messages received and except where specifically authorised by the other person, do not access any other person's in-box or other email folders nor send any email purporting to come from another person.
- 3.1.3 It is good practice to re-read and check an email before sending.
- 3.1.4 If you copy an email to others it may breach the Data Protection Act if it reveals all the recipients' email addresses to each recipient (e.g. in the case of marketing and mailing lists).  
It can also breach duties of confidentiality (e.g. in the case of internal emails to members of a staff benefit scheme). Accordingly, it may be appropriate to use the 'Bcc' (blind carbon copy) field instead of the 'Cc' (carbon copy) field when addressing an email to more than one recipient. If in doubt, seek advice from your line manager.
- 3.1.5 Always check the size of any attachments and try to limit an email attachment/message to a maximum of 15MB (Megabytes) where practical. (Options are available to compress image files, please contact the IT Department for assistance if required). Maximum message size limits are in operation which will stop the sending and receiving of excessively large messages. These will be periodically reviewed in line with business requirements and advised via separate company notices.
- 3.1.6 When sending attachments, such as Word, Excel or PowerPoint, which contain confidential information; files should be protected against unauthorised opening by using a password set via the security features within Microsoft Office. Passwords should be communicated separately to the recipient via phone, text or other methods external to the sending email for security purposes. (Refer also to Security section 6.5)
- 3.1.7 You must not send or circulate internally or externally any information that is defamatory. In particular you must not send or circulate internally or externally any information that contains negative comments

This document is uncontrolled when printed, version control must be assured before use.

# LAND RECOVERY

about an individual or company without first checking that the content of the information is accurate, if in doubt you must check with your manager.

## 3.2 Business use

- 3.2.1 Each business email should include the appropriate Land Recovery Ltd business reference.
- 3.2.2 If the email message or attachment contains information which is time-critical, bear in mind that an email is not necessarily an instant communication and consider whether it is the most appropriate means of communication.
- 3.2.3 If you have sent an important document, you can use the delivery and read receipts to confirm that the email has been received and read.
- 3.2.4 An email message which relates to commercial, contractual, legal customer/client communication must be correctly stored within the email folders/archives, in order to provide a valid audit trail.
- 3.2.5 In light of the security risks inherent in some web-based email accounts, you must not email business documents to your personal web-based accounts. You may send documents to a customer's/client's web-based account if you have the customer's/client's express written permission to do so. However, under no circumstances should you send price sensitive or highly confidential documents to a customer's/clients personal/web-based email account, even if the customer/client asks you to do so. When you need to work on documents remotely they can be saved to a disk or retrieved via remote system access using secure VPN connectivity.

## 3.3 Personal Use

- 3.3.1 Although Land Recovery Ltd email facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on the condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, you can expect very little privacy because Land Recovery Ltd may need to monitor communications for the reasons given in item 9.1.  
You will greatly increase the privacy of any personal email by complying with the procedures set out in item 3.3.3 below.
- 3.3.2 Under no circumstances may Land Recovery Ltd facilities be used in connection with the operation or management of any business other than that of Land Recovery Ltd or a customer/client of Land Recovery Ltd unless express permission has been obtained from your Line Manager or Director.
- 3.3.3 All personal email you send from Land Recovery Ltd facilities must be marked PERSONAL in the subject heading, and all personal email sent or received must be filed in a separate folder marked "Personal" in your inbox should you wish to retain it after reading. Contact IT Support if you need guidance on how to set up and use a personal folder. All email contained in your inbox and your sent items box are deemed to be business communications for the purposes of monitoring (see item 9.4).
- 3.3.4 You must ensure that your personal email use:
  - (a) does not interfere with the performance of your duties
  - (b) does not take priority over your work responsibilities
  - (c) is minimal and limited to taking place substantially outside of normal working hours (i.e. during any breaks which you are entitled to or before or after your normal hours of work)
  - (d) does not cause unwarranted expense or liability to be incurred by Land Recovery Ltd.
  - (e) does not have a negative impact on Land Recovery Ltd in any way; and
  - (f) is lawful and complies with this policy.
- 3.3.5 As with any correspondence made using Land Recovery Ltd electronic facilities, you can delete personal email from the live system, but they will have been copied (perhaps many times) within the data backup / archiving routines and in that form will be retained indefinitely.
- 3.3.6 By making personal use of our facilities for sending and receiving email you signify your agreement to abide by the conditions imposed for their use, and signify your consent to Land Recovery Ltd monitoring your personal email in accordance with item 9 of this policy.

This document is uncontrolled when printed, version control must be assured before use.

# LAND RECOVERY

## 4. USE OF INTERNET AND INTRANET

- 4.1 We trust you to use the internet sensibly. Bear in mind at all times that, when visiting a website, information identifying your PC may be logged. Therefore any activity you engage in via the internet may affect Land Recovery Ltd.
- 4.2 We recognise the need for individuals to have to carry out some personal tasks during working hours, e.g. for internet banking or online shopping, and this is permitted subject to the same rules as are set out for personal email use in item 3.3.4 of this policy. If these activities require additional software to be installed onto your PC then you should submit a request to IT Support who may be able to arrange this for you. Whenever you need to download software to enable you to access an online service you must obtain the express permission via the IT Service Desk who will consider the request in line with Land Recovery Ltd Policy.
- 4.3 You are strongly discouraged from providing your Land Recovery Ltd email address when using public websites for non-business purposes, such as online shopping. This must be kept to a minimum and done only where necessary, as it results in you and Land Recovery Ltd receiving substantial amounts of unwanted email.
- 4.4 Access to certain websites and content types maybe blocked in order to protect employees from inappropriate content. If you have a particular business need to access blocked content, please contact the IT Service Desk who will review your request.

You must not:

- 4.4.1 introduce packet-sniffing or password-detecting software
  - 4.4.2 seek to gain access to restricted areas of Land Recovery Ltd network
  - 4.4.3 access or try to access data which you know or ought to know is confidential
  - 4.4.4 intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software; nor
  - 4.4.5 carry out any hacking activities
  - 4.4.6 Use Land Recovery Ltd systems to participate in any internet chat room or post messages on any external website, including any message board or blog, unless expressly permitted in writing to do so by Land Recovery Ltd.
- 4.5 For your information, breach of items 4.4.1 to 4.4.6 (inclusive) above, would not only contravene the terms of this policy but could in some circumstances also amount to the commission of an offence under the Computer Misuse Act 1990, which creates the following offences:
- 4.5.1 unauthorised access to computer material i.e. hacking
  - 4.5.2 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
  - 4.5.3 Unauthorised access with intent to commit or facilitate commission of further offences.

## 5. MISUSE OF LAND RECOVERY LTD FACILITIES AND SYSTEMS

- 5.1 Misuse of Land Recovery Ltd facilities and systems, including its telephone, email and internet systems, in breach of this policy will be treated seriously and dealt with in accordance with Land Recovery Ltd Disciplinary procedure. In particular, viewing, accessing, transmitting, posting, downloading or uploading any of the following materials in the following ways, or using any of Land Recovery Ltd facilities, will amount to gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):
- 5.1.1 material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive

This document is uncontrolled when printed, version control must be assured before use.

# LAND RECOVERY

- 5.1.2 offensive, obscene, derogatory or criminal material or material which is liable to cause embarrassment to Land Recovery Ltd, and any of its staff or its customers/clients or bring the reputation of Land Recovery Ltd and any of its staff or its customers/clients into disrepute
  - 5.1.3 any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature
  - 5.1.4 any material which, by intent or otherwise, harasses the recipient
  - 5.1.5 any other statement which is designed to cause annoyance, inconvenience or anxiety to anyone
  - 5.1.6 any material which violates the privacy of others or unfairly criticises or misrepresents others
  - 5.1.7 confidential information about Land Recovery Ltd and any of its staff or customers/clients
  - 5.1.8 any other statement which is likely to create any liability (whether criminal or civil, and whether for you or Land Recovery Ltd)
  - 5.1.9 material in breach of copyright and/or other intellectual property rights;
  - 5.1.10 online gambling; or
  - 5.1.11 Unsolicited commercial or advertising material, chain letters or other junk mail of any kind.
- If Land Recovery Ltd has evidence of the examples of misuse set out above it reserves the right to undertake a more detailed investigation in accordance with its disciplinary procedures.

## 6. SYSTEM SECURITY

- 6.1 Security of our IT systems is of paramount importance. We owe a duty to all of our customers/clients to ensure that all of our business transactions are kept confidential. If at any time we need to rely in court on any information which has been stored or processed using our IT systems it is essential that we are able to demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.
- 6.2 Land Recovery Ltd system or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.
- 6.3 Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.
- 6.4 Keep your system passwords safe. Do not disclose them to anyone. Mailbox access can be granted to colleagues without divulging your password using the delegate mailbox option. IT Support will provide guidance on how to do this. If you have disclosed your password to anyone else (e.g. in response to a request from the IT staff) ensure that you change your password once the IT staff no longer need it. Contact IT Support for guidance on how to do this.
- 6.5 If a document is highly commercially confidential contain price sensitive or personally confidential information, you should mark it as "private and confidential" and password-protect the document itself. When sending attachments, such as Word, Excel or PowerPoint, which contain confidential information files should be protected against unauthorised opening by using a password set via the security features within Microsoft Office. Passwords should be communicated separately to the recipient via phone, text or other methods external to the sending email for security purposes.
- 6.6 Copies of confidential information should be printed out only as necessary, retrieved from the printer immediately, and stored or destroyed in an appropriate manner.
- 6.7 You shall not download or install software from external sources if you require additional Software this must be requested via the IT Service Desk.
- 6.8 Only approved company equipment should be connected to laptop and desktop computers. Contact the IT Department for advice before connecting any equipment which may require or prompt for the installation of software.

This document is uncontrolled when printed, version control must be assured before use.

# LAND RECOVERY

- 6.9 External media (USB memory devices, memory sticks, memory cards, portable disk storage, and optical storage media) can provide a convenient means to both backup or transfer data. However, caution should be exercised when these devices / media are used, especially when they have been connected to non Land Recovery Ltd computer equipment or received from a third party. Such devices and media should only be used from trusted sources. Viruses and other malware can inadvertently be introduced using these devices / media. If you are uncertain, please contact the IT Department and request that the media is scanned before connecting or importing into any company device or computer.
- 6.10 Whilst email is scanned by security products for SPAM, viruses and Malware you should always exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious or contains links to suspect web sites. The IT Service Desk should be informed immediately in such circumstances.

## 7. WORKING REMOTELY

- 7.1 This part of the policy and the procedures in it apply to your use of our systems, to your use of our laptops, and also to your use of your own computer equipment or other computer equipment (e.g. client's equipment) whenever you are working on Land Recovery Ltd business away from Land Recovery Ltd premises (working remotely).

When you are working remotely you must:

- 7.1.1 password protect any work which relates to Land Recovery Ltd business so that no other person can access your work
  - 7.1.2 when dealing with commercially sensitive data, position yourself so that your work cannot be seen by any other person
  - 7.1.3 take reasonable precautions to safeguard the security of our equipment, and keep your passwords secret; (e.g. checking the computer screen, when leaving your work area)
  - 7.1.4 inform the police and our IT Department (as appropriate) as soon as possible if either a Land Recovery Ltd laptop in your possession or any computer equipment on which you do Land Recovery Ltd work, even if this is personal IT equipment, has been lost or stolen; and
  - 7.1.5 Ensure that any work which you do remotely is saved on Land Recovery Ltd system or is transferred to our system as soon as reasonably practicable.
- 7.2 Pocket computers, tablet pc's, mobile phones and similar hand-held devices are easily lost or stolen. It is good practice to password-protect access to any such devices used by you on which is stored any personal data of which Land Recovery Ltd is a data controller or any information relating to our business, our clients or their business.

## 8. PERSONAL BLOGS AND WEBSITES

- 8.1 This part of the policy and procedures in it apply to content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content-sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.
- 8.2 Land Recovery Ltd recognise that in your own private time you may wish to publish content on the internet. For the avoidance of doubt, such activities are expressly prohibited during work time or using Land Recovery Ltd systems. The only acceptance to this is if the posting is work related and permission has been granted by your manager.
- 8.3 If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of Land Recovery Ltd staff and/or you discuss your work or anything related to Land Recovery Ltd or its business, customers or staff, Land Recovery Ltd expects you, at all times, to conduct yourself appropriately and in a manner

This document is uncontrolled when printed, version control must be assured before use.



# LAND RECOVERY

which is consistent with your contract of employment and with Land Recovery Ltd policies and procedures. It should be noted that simply revealing your name or usual image of yourself could be sufficient to identify you as an individual who works for Land Recovery Ltd.

- 8.4 If you already have a personal blog or website which indicates in any way that you work for Land Recovery Ltd you should report this to your line manager/departmental head.
- 8.5 If you intend to create a personal blog or website that will say that you work for Land Recovery Ltd or in any way could identify you as someone who works for Land Recovery Ltd then you should report this to your line manager/departmental head.
- 8.6 If a blog posting clearly identifies that you work for Land Recovery Ltd and you express any idea or opinion then you should add a disclaimer such as "these are my own personal views and not those of Land Recovery Ltd "
- 8.7 The following matters will be treated as gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):
  - 8.7.1 Revealing confidential information about Land Recovery Ltd in a personal online posting. This might include revealing information relating to Land Recovery Ltd clients, business plans, policies, staff, financial information or internal discussions. Consult your manager if you are unclear about what might be confidential.
  - 8.7.2 Criticising or embarrassing Land Recovery Ltd, its clients or its staff in a public forum (including any website). You should respect the corporate reputation of Land Recovery Ltd and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague or workplace matter the correct procedure is to raise a grievance using Land Recovery Ltd Grievance procedure.
  - 8.7.3 Accessing or updating a personal blog or website from Land Recovery Ltd computers or during work time.
- 8.8 If you think that something on a blog or a website could give rise to a conflict of interest and in particular concerns issues of impartiality or confidentiality required by your role then this must be discussed with your line manager/departmental head.
- 8.9 If someone from the media or press contacts you about your online publications that relate to Land Recovery Ltd you should talk to your line manager/departmental head before responding and Land Recovery Ltd line manager/department head will contact the Land Recovery Ltd Representative responsible for external communications.
- 8.10 Online publications which do not identify the author as a member of Land Recovery Ltd staff and do not mention Land Recovery Ltd and are purely concerned with personal matters will normally fall outside the scope of Land Recovery Ltd communications policy.

## 9. **MONITORING OF COMMUNICATIONS BY LAND RECOVERY LTD**

- 9.1 Land Recovery Ltd is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. Land Recovery Ltd may monitor your business communications for reasons which include:
  - 9.1.1 providing evidence of business transactions
  - 9.1.2 ensuring that Land Recovery Ltd business procedures, policies and contracts with staff are adhered to
  - 9.1.3 complying with any legal obligations
  - 9.1.4 monitoring standards of service, staff performance, and for staff training
  - 9.1.5 preventing or detecting unauthorised use of Land Recovery Ltd communications systems or criminal activities; and

This document is uncontrolled when printed, version control must be assured before use.

# LAND RECOVERY

9.1.6 Maintaining the effective operation of Land Recovery Ltd communications systems.

9.2 Land Recovery Ltd will monitor telephone, email and internet traffic data (i.e. sender, receiver, subject; non-business attachments to email, numbers called and duration of calls; domain names of websites visited, duration of visits, and files downloaded from the internet) at a network level (but covering both personal and business communications) for the purposes specified at item 9.1. For the purposes of your maintenance of your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you regularly visit websites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By carrying out such activities using Land Recovery Ltd facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

9.3 Sometimes it is necessary for Land Recovery Ltd to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, additional access can be granted through the IT Helpdesk and relevant approvals.

9.4 Any emails which are not stored in your "Personal" folder in your mailbox and which are not marked PERSONAL in the subject heading will be treated, for the purpose of availability for monitoring, as business communications since we will have no way of knowing that they were intended to be personal. Therefore you must set up a rule to automate the routing of personal email to your personal folder – ask IT Support for guidance on how to do this. Furthermore, there is a risk that any person authorised to access your mailbox may have their own preview pane option as a default setting, which would reveal the content of any of your personal email not filed in your "Personal" folder, whether or not such email are marked PERSONAL. It is up to you to prevent the inadvertent disclosure of the content of personal email by filing your personal email in accordance with this policy. In particular, you are responsible to anybody outside Land Recovery Ltd who sends to you, or receives from you, a personal email, for the consequences of any breach of their privacy which may be caused by your failure to file your personal email.

9.5 In certain very limited circumstances we may, subject to compliance with any legal requirements, access email marked PERSONAL. Examples are when we have reasonable suspicion that they may reveal evidence of unlawful activity, including instances where there may be a breach of a contract with Land Recovery Ltd.

9.6 All incoming emails are scanned by content filtering and virus-checking software. The software will also block unsolicited marketing email (spam) and email which have potentially inappropriate attachments. If there is a suspected virus in an email which has been sent to you, the sender will automatically be notified and you will receive notice that the email is not going to be delivered to you because it may contain a virus.

## 10. DATA PROTECTION

10.1 As a member of Land Recovery Ltd who uses our communications facilities, you will inevitably be involved in processing personal data for Land Recovery Ltd as part of your job. Data protection is about the privacy of individuals, and is governed by the Data Protection Act 2018. This Act defines, among others, terms as follows:

10.1.1 "data" generally means information which is computerised or in a structured hard copy form

10.1.2 "personal data" is data which can identify someone, such as a name, a job title, a photograph

10.1.3 "processing" is anything you do with data – just having data amounts to processing; and

10.1.4 "Data controller" is the person who controls the purposes and manner of processing of personal data – this will be Land Recovery Ltd in the case of personal data processed for the business.

10.2 Whenever and wherever you are processing personal data for Land Recovery Ltd you must keep it, confidential and secure, and you must take particular care not to disclose them to any other person, whether inside or outside Land Recovery Ltd, unless authorised to do so. Do not use any such personal data except as authorised by Land

This document is uncontrolled when printed, version control must be assured before use.

# LAND RECOVERY

Recovery Ltd for the purposes of your job. If in doubt advice can be obtained from the Land Recovery HR Manager.

- 10.3 The Data Protection Act gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an email or otherwise. It is another reason why personal remarks and opinions must be made or given responsibly, and they must be relevant and appropriate as well as accurate and justifiable. In the event that information is requested this shall be processed in accordance with Land Recovery Ltd Data Protection Policy.
- 10.4 For your information, section 55 of the Data Protection Act provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of Land Recovery Ltd: you exceed your authority in collecting personal data; you access personal data held by Land Recovery Ltd; to control it or you pass them on to someone else (whether inside or outside Land Recovery Ltd).
- 10.5 While Land Recovery Ltd is a data controller of all personal data processed for the purposes of our business, you will be a data controller of all personal data processed in any personal email which you send or receive. Use for social, recreational or domestic purposes attracts a wide exemption under the Data Protection Act, but if, in breach of this policy, you are using our communications facilities for the purpose of a business which is not Land Recovery Ltd, then you will take on extensive personal liability under the Data Protection Act.
- 10.6 To help you understand and comply with Land Recovery Ltd obligations as a data controller under the Data Protection Act you may be offered, and you may also request, training. Whenever you are unsure of what is required or you otherwise need guidance in data protection, you should consult our the Land Recovery HR Manager/IT Department.
11. **COMPLIANCE WITH THIS POLICY**
- 11.1 Failure to comply with this policy may result in disciplinary action being taken against you under Land Recovery Ltd Disciplinary procedure, which may include summary dismissal, and/or in the withdrawal of permission to use the firm's equipment for personal purposes. If there is anything in this policy that you do not understand, please discuss it with your line manager/departmental head, further advice can be obtained via the Land Recovery HR Manager and IT Department.
- 11.2 Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time. It will also be subject to annual review, in any event the Policy shall be amended along with the publication date. You will be alerted to important changes and updates will be published on our company main drive.

Signed:



Dan Beecroft  
Managing Director  
January 2024

Title:  
Date: