CONTENTS Page

1. POLICY SUMMARY

This policy covers any person using a device owned by someone other than Lodge Security (for example, personal devices) to access data - commonly known as Bring Your Own Device (BYOD).

You must comply with the whole policy, but in summary:

- **You must immediately tell Lodge Security** IT Desk **immediately** with details. If your device is lost, stolen, infected with malware or the security of the device is otherwise compromised
- **Lodge Security does not provide support for the use of personal devices** although FAQs and installation instructions are maintained for your use. Lodge Security will accept comments and issues around BYOD but does not commit to respond to them. Issues with connectivity will be investigated, but if they cannot be reproduced you will have to find solutions in conjunction with your personal providers
- Compliance with this policy is part of your employment contract

2. INTRODUCTION

Lodge Security has a responsibility to safeguard the information that has been provided to them. This policy sets out Lodge Security's approach to ensure that:

- The requirements of UK law on personal data management are being met
- Lodge Security Data Privacy and Information Security policies are being followed
- Where third party data is being used, the requirements of the data owners are being followed

Lodge Security recognises that users may wish to use their own mobile devices to access data and use Lodge Security applications as part of flexible working arrangements. This policy outlines the responsibilities of both Lodge Security and the device owner.

3. PROHIBITED SERVICES AND DATA

Lodge Security reserve the right to prohibit use of personally owned devices (BYOD) for accessing certain category of services and data as necessary.

4. WHO DOES THE POLICY APPLY TO?

This policy applies to all persons who connect or intend to connect a device not owned by Lodge Security to access Lodge Security data.

5. LODGE SECURITYS' RESPONSIBILITES

.

As the data controller, Lodge Security is responsible for ensuring that all processing of personal data which is under its control remains in compliance with UK law. Additionally, Lodge Security receives data from partners which may be restricted by their security policies with which we have to comply.

Lodge Security must also remain mindful of the personal usage of such devices and the privacy of the individual. Technical and organisational measures used to protect our data must remain proportionate to the risks and consider your rights as an individual to privacy.

6. RIGHTS, PRIVILEGES AND RESPONSIBILITIES

The use of a personally owned device in connection with Lodge Security business is a privilege granted to device owners. Lodge Security reserves the right to revoke these privileges without notice.

You must read and understand this policy before configuring your device to access Lodge Security information.

Lodge Security remains the data controller for all Lodge Security related data held on BYODs.

Disciplinary and/or criminal action may be taken if a breach of policy or law occurs. Compliance with this policy is part of your employment contract.

As the device owner, you carry specific responsibilities, as listed below:

- You will not lend anyone your device to access Lodge Security information or use Lodge Security's' infrastructure
- In order to access your Outlook email and calendar, you will need to enter your network account password. You may be required to provide a second authentication factor before access, this will be via either a text message or an app

- You must ensure that your device is compliant, and that security software is kept up to date
- You are responsible for the safekeeping of your own personal data. We recommend that you secure and encrypt your phone appropriately using the facilities on the device, and that you have an up-to-date malware scanning solution installed (anti-virus)
- You must conform strictly to Lodge Security's Data Protection Policy and Information Security Policy for the movement and use of information
- You should install find my roid (android phones) or find my phone (iPhone) application to your phone

All users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, 'jailbreaking' your iPhone or 'rooting' your android device even if this adds additional functionality.

7. WHICH IT SERVICES ARE AVAILABLE?

Currently, the IT Services available and covered by policy are:

- Email
- Calendar
- Contacts
- Tasks
- Instant messaging via Ms Teams
- Collaboration and group discussion via Teams
- Access to ShopSafe – ALERT
- Timegate
- Whatsapp

Note that some file types cannot be securely opened, and hence you may find you cannot open certain attachments. Additionally, mobile software may have different and more limited functionality from desktop versions.

8. WHAT SUPPORT WILL LODGE SECURITY IT PROVIDE?

Lodge Security IT will not support or maintain any personal device.

It is recommended that device owners ensure their device as part of their home contents insurance or via a specific mobile device insurance scheme and advise their insurer that the device will be used for work purposes at home and at work locations.

9. IF A SECURITY INCIDENT SHOULD OCCUR

A security incident is defined as **any** event that could compromise information security. Some examples: your device is lost or stolen, someone else gains access to your password/passcode, your device becomes infected with malware.

If a security incident should occur, you are required to inform Lodge Security IT Desk **immediately** with details.

Note that not reporting security incidents is a breach of the Acceptable Use Policy.

10. GUIDELINES FOR ACCEPTABLE BEHAVIOUR

Be aware that any personal device used at work may be subject to discovery in litigation. This means that it could be used as evidence in a lawsuit against the company. Your data could be examined not only by Lodge Security, but also by other parties in any legal action.

11. ACCESS COMPANY INFORMATION OUTSIDE OF THE EEA

The UK law on data protection only permits export of personal data to certain countries. Because of this please ensure you restrict use of access to company data unless absolutely necessary when outside of the EEA.

12. IF YOU LEAVE LODGE SECURITY EMPLOYMENT

As part of the leaver's process, your access to Lodge Security infrastructure and applications will cease and your device will be de-provisioned.

Device owners bring their devices to use at Lodge Security as their own risk. Device owners are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Lodge Security is in no way responsible for:

- Personal devices that are broken while at work or during work-sponsored activities
- Personal devices that are lost or stolen at work or whilst undertaking work-related activities
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues)
- The management or creation of users own 'cloud' based user accounts, which are required for purchasing software, or backing up data