Title: VALLEY PROVINCIAL LTD BYOD POLICY

Contents

1. Introduction
2. Policy Scope
3. Policy Intent
4. Policy Provisions and Principles
5. User Responsibilities
6. Monitoring and Access
7. Data Protection and BYOD Enforcement

1. Introduction

BYOD Policy

Valley Provincial is committed to meeting its legal and duty of care obligations while at the same time providing a flexible environment to allow the use of non-Valley Provincial owned or issued devices to access corporate systems and store Company information. The use of non-Valley Provincial owned or issued devices for work purposes can be beneficial to Valley Provincial but it also introduces new risks protecting the integrity, confidentiality and availability of Company information. Valley Provincial does not have any control on the security mechanisms implemented on privately owned devices. Therefore, if the device was compromised, lost or stolen there would be a risk that any Company information stored on it could be accessed and exploited by unauthorised individuals.

2. Policy Scope

This policy applies to all Valley Provincial staff, subcontractors and third parties working at Valley Provincial, who use a non-Valley Provincial issued device or their own personal device to process Company data. This is commonly known as “Bring Your Own Device” or BYOD. For the purposes of this guidance personal devices include, but are not limited to home desktop PCs, tablets (iPads etc.), smartphones, laptops, video and audio recording equipment. Some devices may not have the capability to connect to Valley Provincial IT systems. This policy should be read in conjunction with the Data Protection Policy and its supporting policies, procedures and standards.

3. Policy Intent

This policy is produced to provide a clear instruction on how BYOD devices can be used in Valley Provincial to ensure that Valley Provincial complies with data protection legislation and that Company information, confidential, personal and sensitive information, is protected from unauthorised access, dissemination, alteration or deletion.

4. Policy Provisions and Principles

General

The contents of Company systems and Company data remain the property of Valley Provincial. This covers all materials, data, communications and information, including but not limited to, e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device during the course of your work for Valley Provincial or on its behalf is the property of Valley Provincial, regardless of who owns the device.

Company data held on personally owned devices is subject to the Freedom of Information Act and the Data Protection Act and must be processed in compliance with information related legislation and associated Company policies.

Valley Provincial reserves the right to refuse access to personally owned devices or software where it considers that there is a security risk to its systems and infrastructure. While our IT provider (Utilize) will always endeavour to assist colleagues wherever possible, Valley Provincial cannot take responsibility for supporting non-Company managed devices.

5. User Responsibilities

BYOD Policy

All individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of Company information (as well as their own information);
- Invoke the relevant security features for the device.
- Maintain the device themselves ensuring it is regularly patched and upgraded using updates provided by vendors.
- Ensure that the device is not used for any purpose that would be at odds with Valley Provincial IT Regulations of Use especially when it is on site or connected to Valley Provincial network; and
- Pay for their own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs.

Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data.
- Keep information confidential where appropriate.
- Maintain the integrity of data and information, including that on Valley Provincial premises.; and
- Take responsibility for any software they download onto their device.

Staff using BYOD must:

- Set up passwords, passcodes, passkeys or biometric equivalents of sufficient length and complexity for the particular type of device.
- Set up remote wipe facilities if available and implement a remote wipe if they lose the device.
- Ensure that software on personally owned devices is appropriately licenced.
- Encrypt documents or devices as necessary.
- Not hold any information that is sensitive, personal, confidential, or of commercial value on personally owned devices. Instead, they should use their device to make use of the facilities provided to access to information securely over the internet. (More information on determining if information is 'confidential' is available on Valley Provincial's web site);
- Where it is essential that information belonging to Valley Provincial is held on a personal device it should be deleted as soon as possible once it is no longer required, including information contained within emails.
- Ensure that relevant information is copied back onto Company systems and manage any potential data integrity issues with existing information.
- Report the loss of any device containing Company data (including email) to the Directors and Steve Childs immediately.
- Be aware of any Data Protection issues and ensure personal data is handled appropriately.
- Report any security breach immediately to the Directors in accordance with the Data Protection Policy.
- Ensure that no Company information is left on any personal device indefinitely and make sure data is removed before a device is disposed of, sold or transferred to a third party; and
- Not keep any information longer than is necessary and only in line with Company guidelines.

6. Monitoring and Access

BYOD Policy

Valley Provincial will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks or both.
- Prevent a device accessing a particular system; and
- Take all necessary and appropriate steps to retrieve information owned by Valley Provincial.

7. Data Protection and BYOD

Valley Provincial must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 2018. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be always handled with a higher degree of protection.

Valley Provincial, in line with guidance from the Information Commissioner's Office on BYOD, recognises that there are inherent risks in using personal devices to hold personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data. A breach of the Data Protection Act can lead to Valley Provincial facing significant fines. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to Valley Provincial's information being withdrawn, or even a criminal prosecution. For more information see Valley Provincial's Data Protection Policy.

Enforcement

Failure to comply with this policy may result in the revocation of access to Company systems, whether through a personally owned device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, partner or affiliate, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether use of the device takes place at your normal place of work. You are required to co-operate with any investigation into a suspected breach, which may include providing us with access to the device.

By using your device for Company related purposes and unless otherwise agreed with you in a separate agreement with Valley Provincial, you acknowledge that you alone are responsible for all costs associated with the device and that you understand that your business usage of the device may increase your voice and data usage charges.

Monitoring and review

All aspects of this policy are to be reviewed annually.

Signed: Paul Brown _____

Paul Brown, Managing Director

Date: **16.12.2024** _____

Review date: **16.12.2025** _____