THE ISLE OF GIGHA HERITAGE TRUST

Mobile Device Acceptable Use Policy

Author signature

Date 12.06.2020

Chair of IGHT Board signature

Date 16-06-2020

Revision History

Version	Section	Page	Detail Amended	Amended By	Date
1	All	All	New policy for GDPR compliance	S Bannatyne	April 2020

Contents

Introduction

This policy has been created for compliance with the General Data Protection Regulation 2018.
The Isle of Gigha Heritage Trust may issue employees with a laptop for use only pertaining to the business of the organisation and its subsidiary companies.
This policy outlines the responsibilities of both the employer and the users of company owned devices.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of IGHT.
- Employees should only access websites relevant to the activities that directly or indirectly support the business of IGHT.
- Devices' camera and/or video capabilities may be enabled for activities that directly or indirectly support the business of IGHT.
- Devices may not be used at any time to:
  - View, store or transmit illicit materials
  - View, store or transmit proprietary information belonging to another company
  - Harass others
  - Engage in outside business activities
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- IGHT has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Technical Support

- Where remote connection to the company server is necessary this will be authorised by the IT support company used by IGHT.
- Connectivity issues are supported by IT; employees should not contact the device manufacturer for operating system or hardware-related issues.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network, if applicable.

Security

- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- A strong password consists of at least six characters and a combination of upper- and lower-case letters, numbers and symbols.
- The device must lock itself with a password or PIN if it is idle for five minutes.
- After five failed login attempts, the device will lock. Contact IT to regain access.
- Do not open any emails or weblinks that you are not expecting or recognise or suspect to be malicious.
- If you suspect that the device has been subject to a virus, malware, ransomware or any irregularity, this must be reported to IT support immediately.

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- Lost or stolen devices must be reported to the company within 24 hours.
- The company reserves the right to disconnect devices or disable services without notification.
- The employee is expected to use the company device in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- IGHT assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- IGHT reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Please also refer to the 'Bring Your Own Device Policy' for employee / director owned devices.