THE ISLE OF GIGHA HERITAGE TRUST

GDPR: Data Breach Precautions 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

Introduction
This document has been created for compliance with the General Data Protection Regulation 2018 (GDPR).

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

As part of IGHT's role in complying with the GDPR principles, all reasonable precautions must be taken to avoid the loss or misuse of personal data, which is classed as a data breach. All data breaches must be reported to the Information Commissioners' Office within 72 hours and reported to all data subjects who may be affected. The ICO will assess the seriousness of the data breach and may launch an investigation. This may result in a fine or a 'cease processing' order.

All directors and employees are advised of the following actions in order to prevent a data breach:

- Use PIN numbers / passwords where necessary to lock mobile phones; tablets; laptops; personal computers.
- Log out of email accounts after use.
- Log out of online bank accounts after use.
- Log out of financial software systems after use e.g. Sage, Xero.
- Log out of apps after use e.g. Facebook; Free to Book; Booking.com
- Do not store passwords for automatic log in.
- Change your passwords regularly.
- Delete email chains where appropriate - opinions are also classed as data.
- Delete emails with attachments that contain personal data e.g. CVs, HR related documents.
- Do not keep emails for longer than is necessary.
- Directors should make arrangements with office staff to store relevant email attachments on the company server only.
- When sending an email make sure you are sending it to the correct address. An email sent to an incorrect address is classed as a data breach.
- Check who is copied in when replying to an email so that only intended recipients are sent the email.
- Telephone and video conference calls must be held in private.
- Consider the background visible to other participants when on a video conference call.
- Employees must follow a 'clear desk' policy to prevent unintentional disclosure of data to visitors and office cleaners.
- Empty the 'Deleted' folder on your email account regularly.

- Empty the 'Recycling Bin' on your PC / laptop regularly.
- Do not save documents to the desktop on your PC or laptop; use the company server only to store company documents.
- When printing ensure that all documents have been retrieved from the printer. If there is a paper jam, take action to delete the printing job if possible, to avoid the documents being collected by an unintentional recipient when printing resumes.
- Shred confidential documents rather than disposing of them in the waste bin.
- Do not keep data longer than is outlined in the Retention Policy.
- If your mobile phone / laptop / tablet is lost or stolen this is classed as a data breach.
- If documentation belonging to IGHT or a subsidiary company containing personal data is lost or stolen this is classed as a data breach.
- Data breaches must be reported to the chairperson and/or your line manager immediately.

Contact details for ICO:

The Information Commissioner's Office

45 Melville Street

Edinburgh

EH3 7HL

Telephone: 0303 123 1115
Email: Scotland@ico.org.uk