Risk Management and Policies

Acceptable Use Policy

This forms part of the Fèisean nan Gàidheal policy portfolio

Date Approved	04/03/2022
Purpose	To cover the security of Fèisean nan Gàidheal's information and IT equipment.
Summary	Information and policies around secure use and storage of information, including IT.

Fèisean nan Gàidheal

Acceptable Usage Policy

This Acceptable Usage Policy covers the security and use of Fèisean nan Gàidheal's information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Fèisean nan Gàidheal's (hereafter referred to as 'we/our') employees, contractors and agents (hereafter referred to as 'you/your).This policy applies to all information, in whatever form, relating to our activities, and to all information handled by us relating to other organisations with whom we deal.

1. Computer Access Control

Your Responsibility

Access to our IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, you are accountable for all your actions on our IT systems.

You must not:

- Allow anyone else to use your user ID and password on our system.
- Leave your user accounts logged in at an unattended and unlocked computer. (Press Windows + L to lock your computer).
- Use someone else's user ID and password to access our IT systems.
- Leave your password unprotected (for example writing it down).
- Perform any unauthorised changes to our IT systems or information.
- Attempt to access data that you are not authorised to use or access.
- Exceed the limits of your authorisation or specific business need to interrogate the system or data.
- Connect any non-FnG authorised device to our network or IT systems.
- Store our data on any non-authorised equipment.
- Give or transfer our data or software to any person or organisation, outside Fèisean nan Gàidheal, without our authority. (Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.)

2. Internet and email Conditions of Use

Use of our internet, including social media and email, is intended for business use. Personal use is permitted where such use does not affect your work performance, is not detrimental to us in any way, not in breach of any term and condition of employment and does not place you or Fèisean nan Gàidheal in breach of statutory or other legal obligations.

You are accountable for your actions on the internet and email systems. You must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which we consider offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.

- Post any information on the internet that relates to us, alter any information about us, or express any opinion about us, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward our emails to personal email accounts.
- Post inappropriately on social media.
- Make official commitments through the internet or email on our behalf unless authorised to do so.
- Download copyrighted material such as music media files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the relevant member of staff.
- Connect our devices to the internet using non-standard connections.

3. Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, we enforce a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.
- Electronic files should be stored in accordance with our GDPR policy and disposed of as appropriate.

4. Working Off-site

When working remotely with our devices (e.g. laptops), the following controls must be applied:

- Working away from the office must be in line with our remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones and tablets. They must be protected at least by a password or a PIN and, preferably, by encryption.

5. Mobile Storage Devices

Mobile devices (including USB drives) must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only our authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

You must not store personal files on our IT equipment.

6. Viruses

Centralised, automated virus detection and virus software updates are set up within the our devices.

All computers have antivirus software installed to detect and remove any virus automatically. Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved our anti-virus software and procedures.

7. Monitoring and Filtering

All data that is created and stored on our computers is the property of Fèisean nan Gàidheal. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy, including GDPR.

We have the right (under certain conditions) to monitor activity on our systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

This policy must be read in conjunction with:

- Data Protection Policy
- Remote working policy

It is your responsibility to report suspected breaches of security policy without delay to your line management or another relevant member of the team.All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with our disciplinary procedures.