Risk Management and Policies

Data Protection Policy

This policy forms part of the Fèisean nan Gàidheal policy portfolio

Date Approved	23.02.2018
Purpose	To comply with relevant legislation in respect of the personal data Fèisean nan Gàidheal holds about individuals, follow comprehensive but proportionate governance measures and protect the organisation from the consequences of a breach of its responsibilities.
Summary	Responsibilities and measures to ensure security of data held by Fèisean nan Gàidheal and members, including purposes for which data can be held, for how long, and identification of key risks.

Fèisean nan Gàidheal
Data Protection Policy

Data Controller (Organisation)
Fèisean nan Gàidheal, Meall House, Portree, Isle of Skye, IV51 9BZ
Office of the Information Commissioner Registration Number Z7084687

Scope of policy
This policy covers all personal data/information processed by the organisation and applies to:
- all offices and officers of Fèisean nan Gàidheal
- Fèisean nan Gàidheal's Board of Trustees
- consultants and self-employed administrators contracted by Fèisean nan Gàidheal.

Where individual Fèisean are registered with the Office of the Information Commissioner, Fèisean nan Gàidheal's registration will not apply to them, except in the case of joint data. Member Fèisean, not already registered as data controllers, may adopt or adapt this policy for their own purposes.

Purpose of policy
The purpose of this policy is to enable Fèisean nan Gàidheal to:
- comply with relevant legislation in respect of the data it holds about individuals
- follow good governance measures
- protect the organisation from the consequences of a breach of its responsibilities.

Policy statement
From 25 May 2018 the EU General Data Protection Regulation (GDPR) will become law within the United Kingdom. All organisations currently subject to the Data Protection Act 1998 (DPA) must comply with the GDPR by that date.

The GDPR will replace the current DPA and is intended to update the legislation to take account of changing technologies and the ways in which citizens now engage with organisations.

The UK Government is expected to pass a new Data Protection Bill and has indicated that, once it becomes law, its intention is to ensure the standards required by GDPR will remain in place in the UK post-Brexit.

Fèisean nan Gàidheal will:
- implement appropriate technical and organisational measures as well as providing support for staff and volunteers who handle personal data, so that they can act confidently, consistently and transparently in minimising and, where appropriate, pseudonymising data
- maintain relevant documentation on data processing activities
- use data protection impact assessments where appropriate
- appoint a Data Protection Officer to raise awareness of this policy within the organisation and offer support in its implementation.

Brief introduction to the General Data Protection Regulation (GDPR)
Many of the GDPR's concepts and principles will be the same as the DPA, but there are some new elements and significant enhancements.

The GDPR provides the following rights for individuals:
1. The right to be informed which encompasses our obligation to provide 'fair processing information' typically through a privacy notice. It emphasises the need for transparency over how we use personal data.
2. The right of access, offering individuals a right to access personal data and supplementary information. This will, generally, be free of charge and the deadline for making it available will be reduced to one month instead of 40 calendar days. It will be possible for us to charge for repeated requests and to refuse to comply with requests that are unreasonable
3. The right to rectification enabling individuals to have personal data rectified if it is inaccurate or incomplete. Under DPA this was an issue for the courts. Under GDPR the ICO will be the enforcer.
4. The right to erasure, also known as 'the right to be forgotten', whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing.
5. The right to restrict processing, whereby individuals may 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it.

6. The right to data portability which allows individuals to obtain and reuse their personal data for their own purposes across different services, when processing is carried out by an automated means.
7. The right to object, whereby individuals may object to processing based on legitimate interests.
8. Rights related to automated decision-making including profiling.

The GDPR requires that any personal data held should be:
- Processed only for specified, explicit and legitimate purposes
- Processed fairly, lawfully and transparently
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Kept for no longer than is necessary where data subjects are identified
- Processed securely and protected against accidental loss, destruction or damage.

Purposes for which personal data may be held
Personal data relating to employees may be collected primarily for the purposes of:
- recruitment, promotion, training, redeployment, and/or career development
- administration and payment of wages and sick pay
- calculation of certain benefits including pensions
- disciplinary or performance management purposes
- performance review
- recording of communication with employees and their representatives
- compliance with legislation
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and educational courses and/or to assist future potential employers
- staffing levels and career planning

The organisation considers that the following personal data falls within the categories set out above:
- personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant
- references and CVs
- emergency contact details
- notes on discussions between management and the employee
- appraisals and documents relating to grievance, discipline, promotion, demotion, or termination of employment
- training records
- salary, benefits and bank/building society details
- absence and sickness information
- pension information

Employees will be informed about data protection issues, and their rights to access their own personal data, through the Employee Handbook. Employees, or potential employees, will be advised of the personal data which has been obtained or retained, its source, the purposes for which the personal data may be used, or to whom it may be disclosed. The organisation will regularly review the nature of the information collected and held to ensure there is a sound business reason for requiring the information to be retained.

Retention of Records
The organisation follows the retention periods recommended by the Information Commissioner in its Employment Practices Data Protection Code. These are as follows, in the absence of a specific business case supporting a longer retention period.

Data Type	**Retention period**
Application form	Duration of employment
References received	1 year
Payroll and tax information	6 years
Personnel records	6 years
Records relating to accident or injury at work	3 years from date of last entry in accident book

Managers must ensure that the Data Protection Officer is informed of any changes in their uses of personal data that might affect the organisation's notification to the ICO.

Key Risk
Fèisean nan Gàidheal has identified personal data breach as a potential key risk, which this policy is designed to mitigate. A personal data breach means a breach of security leading to accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Fèisean nan Gàidheal MUST report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. The ICO has the power to impose fines up to of €20 million or 4% of annual turnover.

Security
Security must not be confused with confidentiality. Confidentiality is concerned with the level of information which may be divulged. Security maintains those boundaries.

Fèisean nan Gàidheal will:

- Carry out a risk assessment of data systems and act on results on an annual basis
- Maintain up-to-date security systems (for example using firewalls and encryption technology)
- Restrict access to personal data to those that need it
- Train staff on data security
- Review data security regularly

Responsibilities

Trustees
The Board of Trustees recognises its overall responsibility for ensuring that Fèisean nan Gàidheal complies with its legal obligations.

Data Protection Officer
The Data Protection Officer has the following responsibilities:

- Briefing the Trustees on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification of data breaches

Specific Responsibilities of Staff
The Chief Executive, Executive Manager, Development Manager and Fèisgoil Manager may:

- Handle subject access requests (SAR's)
- Approve unusual or controversial disclosures of personal data

All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. It should be noted that data processed in connection with Fèisean nan Gàidheal's PVG scheme is retained separately and disclosure records are only accessible to the Collator and the Chief Executive.

Where Fèisean adopt or adapt this policy, each Fèis committee becomes responsible for their compliance with this policy.

Enforcement
Significant breaches of this policy, if appropriate, will be handled under Fèisean nan Gàidheal's disciplinary procedures. Compliance with this policy is a condition of employment and any deliberate breach of this policy will result in disciplinary action which may include dismissal and possible legal action.

Guidance
Further guidance on the processing of data may be requested from our Data Protection Officer by e-mailing dpo@feisean.org, and our privacy notice is available at feisean.org/en/privacy-notice/.