Data Protection Policy

(updated July 2017)

Fèis Rois
16-17 High Street
Dingwall
IV15 9RU
feisrois.org

Fèis Rois Data Protection Policy
Data Controller (Organisation) Fèis Rois, 16-17 High Street, Dingwall, IV15 9RU
(Office of the Information Commissioner Registration Number Z1112369)
Registration expiry date: 7 November 2018

Scope of policy

This policy applies to:
- the office of Fèis Rois
- all staff of Fèis Rois
- the Board of Directors
- consultants and self-employed administrators retained by Fèis Rois

Fèisean nan Gàidheal and Fèis Rois act as joint Data Controllers in respect of some of the data referred to here.

Purpose of policy

The purpose of this policy is to enable Fèis Rois to:
- comply with the law in respect of the data it holds about individuals
- follow good practice
- protect Fèis Rois' participants, supporters, staff and other individuals
- protect the organisation from the consequences of a breach of its responsibilities

Policy statement

Fèis Rois will:
- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

Fèis Rois recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:
- keeping information securely in the right hands
- holding good quality information

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, Fèis Rois will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

The General Data Protection Regulation (GDPR) is due to come into force on 25 May 2018 and changes to legislation are noted at the appropriate points below.

Brief introduction to Data Protection Act 1998

The Data Protection Act requires anyone who handles personal information to comply with a number of important principles. It also gives individuals rights over their personal information. The Data Protection Act 1998, and subsequent updates, protect individuals against the misuse of personal data, and covers both manual and electronic records.

Data Protection Principles – Summary

The Act requires that any personal data held should be:
- Fairly and lawfully processed
- Processed only for specified and lawful purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection.

Personal data

This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of 'data' in the Act. Staff will be informed about data protection issues, and their rights to access their own personal data through the Employee Handbook.

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

Employees or potential employees will be advised of the personal data which has been obtained or retained, its source, and the purposes for which the personal data may be used or to whom it will be disclosed. The organisation will review the nature of the information being collected and held on an annual basis 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 period.

Document	**Retention period**
Application form	Duration of employment
References received	1 year
Payroll and tax information	6 years
Sickness records	3 years
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given/information to enable references to be provided	5 years from reference/end of employment
Summary of record of service, e.g. name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years

Key risks

Fèis Rois has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately)
- Insufficient clarity about the range of uses to which data will be put - leading to Data Subjects being insufficiently informed
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access
- Failure to establish efficient systems of keeping personal data up-to-date
- Harm to individuals if personal data is not up-to-date
- Insufficient clarity about the way sessional workers' (e.g. tutors and supervisors, or other short contracts) or volunteers' personal data is being used e.g. given out to general public
- Data Processor contracts

Security

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

Members of staff and volunteers with responsibility for the maintenance of personal records including mailing and participant lists must ensure that the information is kept secure, whether by lock and key in a filing cabinet, and/or by password protection of desktop and laptop computers and portable disks and drives.

Care should also be taken when answering telephone queries requesting addresses, telephone numbers, etc for individuals. A possible compromise is to take the caller's details and pass those to the individual concerned and ask them to make contact. Personal details such as home addresses and telephone numbers should not be divulged unless express permission has been given by the individual (e.g.: staff member working from home, freelance tutor etc).

Advice should be sought from the Data Protection Officer if in doubt as to what information may be given.

Subject Access Requests (see attached Appendix 2) are dealt with by the Chief Executive.

Information required in connection with the Disclosure Scotland scheme is retained separately from other data, and is only accessed by the collator. (See attached Appendix 3)

Responsibilities

The Board of Directors
The board recognises its overall responsibility for ensuring that Fèis Rois complies with its legal obligations.

Data Protection Officer
The Data Protection Officer is currently Alison Lewis (and then Fiona Dalgetty from 30 March 2018), with the following responsibilities:

- Briefing the board 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

Specific responsibilities of other staff:

- Handling subject access requests
- Approving unusual or controversial disclosures of personal data

Team/Department managers
Each team or department where personal data is handled is responsible for drawing up its own operational procedures (including induction and training requests) to ensure that good Data Protection practice is established and followed.

Staff and Volunteers
All staff and volunteers 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.

Enforcement

Significant breaches of this policy will be handled under Fèis Rois' 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.

If you access another employee's records without authority this will be treated as gross misconduct and is a criminal offence under the Data Protection Act 1998, section 55.

Appendix 1 (to Data Protection Policy)

Data Protection Good Practice Note

Taking Photographs in Schools (from Information Commissioner's Office)
This Good Practice Guidance is aimed at Local Education Authorities and those working within schools, colleges and universities. It gives advice on taking photographs in educational institutions and whether doing so must comply with the Data Protection Act 1998.

Recommended Good Practice
The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.
- Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken.
- Photos taken purely for personal use are exempt from the Act.

Examples

Personal use:
- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.
- Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.

Official school use:
- Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.
- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This is unlikely to be personal data and the Act wouldn't apply.

Media use:
A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

Further Information

If you require any further information about this or any other aspect of Data Protection, please contact the ICO using the details below:
Web: www.ico.gov.uk |Email: mail@ico.gsi.gov.uk |Telephone: 01625 545700

Appendix 2 (to Data Protection Policy)

Subject Access Requests (from the website of the Information Commissioner's Office – www.ico.gov.uk)
Checklist for handling requests for personal information (subject access requests)

This guidance aims to assist small and medium sized organisations that receive requests for information covered by the Data Protection Act 1998 (the Act). Individuals have a right under the Act to make a request in writing for a copy of the information you hold about them on computer and in some manual filing systems. This is called a subject access request.

They are also entitled to be given a description of the information, what you use it for, who you might pass it on to, and any information you have about the source of the information.

Organisations have been dealing with requests from individuals for many years, certainly well before there was a formal right of access. Where you are happy to provide the information requested it often makes sense to do so as part of your normal course of business, rather than treating any written request for personal information as a formal request under the Act. At other times you will need to consider the request in the light of the specific provisions of the Act.

This simple checklist should help you deal with subject access requests.

1 Is this a subject access request? Determine whether the person's request will be treated as a routine enquiry or as a subject access request. Any written enquiry that asks for information you hold about the person making the request can be construed as a subject access request, but in many cases there will be no need to treat it as such.

If you would usually deal with the request in the normal course of business, do so. Examples of such requests might be:
- "I've lost the guarantee number for my fridge. Can you tell me what it is, please?"
- "How many cash withdrawals did I make from my account last month?"

The following are likely to be treated as formal subject access requests.
- "Please send me a copy of my staff records."
- "I have a right to see all the invoices issued to me for the last three years. Please send copies to me."
- "I am a solicitor acting on behalf of my client and request a copy of his medical records. An appropriate authority is enclosed."

If you are in any doubt how to respond, go back to the individual or their representative and clarify the situation. Train your staff so they are able to recognise subject access requests when they receive them and know what to do.

No: Handle the query as part of your normal course of business. Yes: Go to 2.

2 Do you have enough information to be sure of the requester's identity?

Often you will have no reason to doubt a person's identity. If you have good cause to doubt the requester's identity you can ask them to provide any evidence you reasonably need to confirm it.

For example, you may ask for a piece of information held in your records that the person would be expected to know, such as membership details, or a witnessed copy of their signature.

Once satisfied, go to 3. Yes: Go to 3.

3 Do you need any other information to find the records they want?

No: Go to 4.
Yes: You will need to ask the individual promptly for any other information you reasonably need to find the records they want. You might want to ask them to narrow down their request. For example, if you keep all your customers' information on one computer system and your suppliers' information on another, you could ask what relationship they had with you. Or, you could ask when they had dealings with you. However, they do have the right to ask for everything you have about them and this could mean a very wide search. You have 40 calendar days to respond to a subject access request after receiving any further information you need and any fee you decide to charge.
(Under the GDPR, your organisation must respond to SARs within one month of receipt. This deadline can be extended by a further two months where there are a number of requests or the request is complex but you must contact the individual within a month of receipt, explaining why the extension is necessary.)

Go to 4.

4 Are you going to charge a fee?

No: Go to 5.
Yes: If you need a fee you must ask the individual promptly for one. The maximum you can charge is £10 unless medical or education records are involved (see guidance on our website).
(Under the GDPR, a request for personal information is free unless the request is 'manifestly unfounded or excessive.' Your organisation can charge a 'reasonable fee' for multiple requests.)

The time in which you must respond starts when you have received the fee and all necessary information to help you find the records.
Go to 5.

5 Do you hold any information about the person?
No: If you hold no personal information at all about the individual you must tell them this.
Yes: Go to 6.

6 Will the information be changed between receiving the request and sending the response?
No: Go to 7.
Yes: You can still make routine amendments and deletions to personal information after receiving a request. However, you must not make any changes to the records as a result of receiving the request, even if you find inaccurate or embarrassing information on the record.

Go to 7.

7 Does it include any information about other people?
No: Go to 8.
Yes: You will not have to supply the information unless the other people mentioned have given their consent, or it is reasonable to supply the information without their consent. Even when the other person's information should not be disclosed, you should still supply as much as possible by editing the references to other people. To help you on this point we have published more detailed guidance on dealing with subject access requests involving other people's information.
Go to 8.

8 Are you obliged to supply the information? There may be circumstances in which you are not obliged to supply certain information. Some of the most important exemptions apply to:
- crime prevention and detection
- negotiations with the requester
- management forecasts
- confidential references given by you (but not ones given to you)
- information used for research, historical or statistical purposes
- information covered by legal professional privilege

No: If all the information you hold about the requester is exempt, then you can reply stating that you do not hold any of their personal information that you are required to reveal.
Yes: Go to 9.

9 Does it include any complex terms or codes? The information may include abbreviations or technical terms that the individual will not understand, for example, '02' means a monthly account, '03' means 'paying on receipt of goods' and so on.
No: Go to 10.
Yes: You must make sure that these are explained so the information can be understood. Go to 10.

10 Prepare the response
A copy of the information should be supplied in a permanent form except where the individual agrees or where it is impossible or would involve undue effort. This could include very significant cost or time taken to provide the information in hard copy form. An alternative would be to allow the individual to view the information on screen.

More information
If you need any more information about this or any other aspect of data protection, please contact the ICO.
Phone: 08456 30 60 60 | 01625 54 57 45
E-mail: please use the online enquiry form on our website
Website: www.ico.gov.uk

Appendix 3 (to Data Protection Policy)

Policy on the Secure Handling, Use, Storage and Retention of Disclosure Information In accordance with the Code of Practice published by the Scottish Ministers under section 122 of the Police Act 1997, for registered persons and other recipients of Disclosure Information, Fèis Rois will ensure the following practice.

1 Disclosures will only be requested when necessary and relevant to a particular post and the information provided on a disclosure certificate will only be used for recruitment purposes.
2 Fèis Rois will ensure that an individual's consent is given before seeking a disclosure, and will seek their consent before disclosing information for any purpose other than recruitment.
3 Disclosure information will only be shared with those authorised to see it in the course of their duties.
4 Where additional disclosure information is provided to Fèis Rois and not to the disclosure applicant, Fèis Rois will not disclose this information to the applicant, but will inform them of the fact that additional information has been provided, should this information affect the recruitment process.
5 Disclosure information will be stored in a locked non-portable container, for a maximum of 6 months. Only those authorised to see this information in the course of their duties will have access to this container.
6 Disclosure information will be destroyed by shredding.
7 No image or photocopy of the disclosure information will be made, however the following details will be retained:

- Date of issue of disclosure
- Name of subject
- Disclosure type
- Position for which disclosure was requested
- Unique reference number of disclosure
- Recruitment decision taken

8 Fèis Rois will ensure that all staff with access to disclosure information are aware of this policy and have received relevant training and support.
9 Fèis Rois undertake to make a copy of this policy and the Code of Practice published by the Scottish Ministers under section 122 of the Police Act 1997 available to any applicant for a post within Fèis Rois that requires a disclosure. Fèis Rois aims through their Equal Opportunities Policy of which this is a part, to ensure that all applicants for positions within the organisation are fairly treated.

Appendix 4 (to Data Protection Policy)

Data Protection Principles

There are eight principles put in place by the Data Protection Act 1998 to make sure that your information is handled properly. They say that personal data must be:

- fairly and lawfully processed
- processed only for specified and lawful purposes
- adequate, relevant and not excessive
- accurate and kept up to date
- not kept for longer than is necessary
- processed in line with your rights
- secure
- not transferred to countries without adequate protection

By law data controllers have to keep to these principles. Fèis Rois (Registration number Z1112369) is registered with the Information Commissioner as a data controller.

Under the GDPR, organisations can withhold personal data if disclosing it would *'adversely affect the rights and freedoms of others.'* It will be up to the UK government to introduce any further exemptions to SARs such as for national security, defence and public security. Charities should take advice if they are proposing to withhold information on this basis as your organisation will need to carefully consider its applicability and its use should not act to result in a refusal to provide all information.