



## Policy #02

### Privacy and Data Protection

***N.B.** Hereafter the Scottish Crofting Federation may be referred to as 'SCF' or simply the 'Federation'*

The Scottish Crofting Federation (SCF) is committed to the privacy of its members, staff, directors, volunteers and representatives in a manner that fosters trust and confidence. This commitment includes protecting the privacy of all the personal information in its care.

Legislation now covering Data Protection is the General Data Protection Regulations (GDPR), which is Europe-wide law, an evolution of the UK's Data Protection Act 1998, and the lawful basis upon which to create a policy for the processing of personal data.

The SCF necessarily holds three types of information which are covered by this policy:

- **organisational** information – publicly available information about the organisation.
- **personal** information – information about individuals, whether SCF members or not; such as names, addresses, ages, telephone numbers and email addresses, for the purposes of internal/external communication, where appropriate.
- **sensitive** personal information – in general this kind of information is only held about employees.

The organisation and people about which SCF holds information are referred to in this policy as **data subjects**.

The SCF will strive for best practice and collect personal data for the legitimate interests of the organisation, whether provided for by GDPR legislation or not; which practice will be covered by this policy within the overarching spirit of the relevant GDPR legislation and the **data subject's** individual rights, as follows:

- the right to be informed; to know what personal data is contained in the organisation's records
- the right to access; to be able to examine the personal data kept by the organisation
- the right to rectification; to correct any mistake or misinformation in the personal data kept by the organisation
- the right to erasure; to delete any personal data kept by the organisation for whatever reason

- the right to restrict processing; to retain it only within the bounds of the organisation and within a permissible time-frame
- the right to data portability; data provided to a controller i.e. derived from an individual's consent for the performance of a contract and when carried out by automated means, where appropriate
- the right to object; to all or some personal data kept by the organisation
- the right not to be subject to automated decision-making, including profiling.

SCF for its part will:

- use personal data fairly, transparently and lawfully;
- collect and retain only information necessary for specific purpose(s) - membership records, financial accountability, trainee and tutor records and case-work records. In addition, it will keep a register of its Council members and the statutory register of its directors.
- ensure the information is relevant, accurate and up-to-date;
- hold only as much as is needed, and only for as long as is needed;
- allow the **data subject**, subject of the personal data held, to inspect, on request, that personal data, in respect to that individual **data subject**;
- keep all personal data secure from unauthorised access.

Designated employees, usually the Membership and Training Administrators respectively are appointed for the time being as SCF **data processors** and given the responsibility of protecting the security of information contained within documents or electronic files in their care.

However, nothing in this policy will preclude INTERNAL 'data sharing' of personal data occurring in the line of normal SCF business and, may be permissible at the instance of an appointed SCF Case Worker or SCF Financial Administrator but only sufficient for the particular purpose or, in response to a particular event associated with that assumed role of Case Worker or Finance Administrator; providing, in each case, an undertaking is made by the appointed persons concerned to the effect that such information is removed and deleted from all forms of their stored electronic or other means of retention (hard copy, electronic or otherwise) when such need has been accomplished and/or, immediately upon cessation of that appointment as Federation Case Worker or Finance Administrator - as the case may be.

Subject to the following limitations:

- SCF will only hold and retain personal information for the purposes for which it was originally collected,
- other purposes to which the **data subject** has knowledge and has expressly given their consent,
- as required or permitted by a lawful authority e.g. Companies House, OSCR, cause of justice i.e. Police, HMRC and/or Court of law.

- except as required by lawful authority, it will not hold or disclose information about individuals without their prior knowledge and explicit consent.

SCF will protect organisational, personal (**Data Subjects**) or sensitive information it holds with security safeguards that are pertinent to the sensitivity of the information and to protect it from unauthorised access, release or use.

SCF will only hold information for specific purposes. It will inform **data subjects** what those purposes are (Fair Processing Notice). It will also inform them when/if those purposes change. Information will not be retained once it is no longer required for the stated purpose and not normally exceeding a period of six (6) years permitted under GDPR or a total of seven (7) years under requirements of Her Majesties Revenue & Customs.

SCF will seek to maintain accurate information by creating ways in which data subjects can update their information held. **Data subjects** will be entitled to have access to information held about them by SCF.

**Data subjects** will be given the option not to receive marketing mailings from SCF and/or its Training Provider or, any other organisation – commercial or otherwise.

Information about **data subjects** will not be disclosed to other organisations or to individuals, except in circumstances where this is a legal requirement or where there is explicit consent or, where the information is publicly available elsewhere.

However, requests for information likely to lead to the identity of a member or former member received from anyone (corporate, individual or legal enforcement), will be assessed by the **data controller**, appointed for the time being, on the merits of the request. SCF's **data controller** will monitor and review SCF's ongoing compliance with the relevant GDPR legislation contemporaneously with this internal policy from time-to-time, being no greater than annually.

Where the **data processor** concerned has doubt or uncertainty about the *bona-fides*, legitimacy or purpose of a request, the **data processor** will seek a decision, based on lawful and legitimate disclosure from the **data controller** - usually the Chief Executive as his/her first-line manager before any such disclosure is made. A record of the request and its eventual determination will be made by the **data processor** at the conclusion stating, in each case, what the determination of the request was and under whose authority it was resolved.

SCF has procedures and infrastructure in place for ensuring the security of all personal data. When no longer required for the purpose to which it was gathered, all records containing personnel data, whether held in document or electronic form, are to be disposed of in an appropriate and secure way.

At the beginning of any project or activity the member of staff, manager or

principal contractor associated with that project will consult the **data controller** about any implications likely to affect the validity of SCF data protection or privacy processes that may arise from the project or its activity. The principal contractor will nominate its own **data processor** and all those persons under his/her control are required to fully conform with the provisions set-out in both GDPR and this policy.

#### **PARLIAMENTARY CROSS-PARTY GROUP ON CROFTING**

*Notwithstanding the provisions cited heretofore in this Policy, the Scottish Crofting Federation is, for the time being, appointed by the Scottish Parliament to the position of Secretariat to the 'Cross-Party Group on Crofting'. In this capacity, the designated Secretary of the group is the group **Data Controller**, to which position is entrusted the security of its members - **Data Subjects** - personal identity, together with that respective member's email address. These personal details are held for the legitimate purposes of communicating by email notices, calling of meetings and transmission of related documents.*

*The Secretariat is not authorised for, nor does it hold, other Personal or any Sensitive data on members of the group. If such a member receives email communication concerning the business of the Cross-Party Group but wants to be removed from the official list of members, the member in question must cause the Secretariat to be advised of the fact forthwith, by any expedient means.*

*In furtherance of the designated Secretary's duty, a record (narrative Minutes) is made of the proceedings of the group's meetings, which may include a list of its members attending meetings of the group to which may also be added action points against that member's name. The approved record is subsequently posted on the Scottish Parliament website.*

When deciding whether to enter into an internal arrangement to share personal data (either as a provider, a recipient or both) there is a foremost requirement to identify the objective and the purpose that it is meant to achieve. Regard should also be given to the potential benefits and risks to an individual or the organisation by sharing that data. Assessing the likely results of NOT sharing that data should be considered equally.

All staff, whether employed full or part-time, together with others likely to encounter SCF personal data information i.e. Case Workers, Board and Council members, will be given training on SCF's privacy and data protection policy and procedures.

SCF shall have in place the means to prevent, insofar as can be reasonably attained, arrangements in place to ensure its cyber security and measures to counter unlawful hacking and/or cyber-attack of its data and other records held either in document, electronically or by other forms are protected.

SCF will carry out a review of its privacy and data protection policy and procedures from time to time, usually once in every calendar year.