Skin Conditions Campaign Scotland

Data Protection Policy

Explanation

Skin Condition Campaign Scotland (SCCS) needs to keep certain information on its employees, freelance staff, members, volunteers, advisors and trustees to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers employed staff, freelance staff, trustees and volunteers.

Definitions

In line with the Data Protection Act 1998 principles, SCCS will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive

- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code[i] suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

Type of Information Processed

SCCS processes the following personal information:

Members:

- Full name
- Email address
- Condition (if they wish)
- Special Areas of Interest, e.g.
    - Campaigning
    - Events
    - New treatment and healthcare information

- Research
- E-Health Solutions
- Evaluation data (gathered on a separate form, so that individuals cannot be identified):
- Ethnicity
- Age range

Personal information is kept in the following forms:

- Electronic information is kept on a password protected computers, one of which is stored in a locked space in our Glasgow office when it is not being used. The second machine is kept by our freelance staff member, and is password protected.
- A back up disc is kept, and is updated monthly. This contains all of the information from the password protected computer, and is also kept in a locked cupboard in the Glasgow office
- Hard copy information is rarely created and never taken outside of SCCS office bases. Please note: both staff use home offices to meet the demands of their roles, in addition to the Glasgow office.

Groups of people within the organisation who will process personal information are: - employed staff, freelance staff, trustees and volunteers.

Notification

SCCS has been advised by the Information Commissioner's Office that we are liable for an exemption, due to the nature of our work. This has been agreed at Board level, but is subject to review when we review our Data Protection policy.

Responsibilities

Under the Data Protection Guardianship Code, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of SCCS, this is the Board of Trustees.

The Board of Trustees delegates tasks to the Data Controller. The Data Controller is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures
- reporting any breaches to the Information Commissioner's Office within 72 hours of this happening as required in the new regulations coming into force on 25 May 2018.

All employed staff, freelance staff, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles. Breach of this policy will result in disciplinary action, in line with the staff handbook.

Policy Implementation

To meet our responsibilities staff, freelancers, volunteers and trustees will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.

Training

Training and awareness raising about the Data Protection Act and how it is followed in this organisation will take the following forms:

On induction: new staff and freelancers will receive a copy of the Staff Handbook (currently in development, July 2016).

General training/ awareness raising: e.g. training led by SCVO in October 2016 on changes to the Data Protection Act. There will be new regulations which apply from 25 May 2018 which will replace the EU Directive 95/46/EC and the Data Protection Act 1998, the finalised details of these regulations are awaited and this document will be updated in accordance with these.

Gathering and Checking Information

Before personal information is collected, we will consider the uses for this information, outlined below.

We will inform people whose information is gathered about the following:

Information requested	Rationale for information requested
Full name	To maintain contact
Email address	To maintain contact
Postcode	To ascertain region (in case regional work becomes relevant in the future)
Condition (optional)	So that people can be notified of condition-specific training and events, to be asked to take part in campaigns and information gathering (e.g. learning from patients' expertise)
Special areas of interest e.g. ● Campaigning ● Events ● New treatments ● Research ● Electronic health solutions ● etc.	This will enable us to develop the work of the organisation in line with the interests of members.
Equalities Monitoring Information (to be gathered separately so that the individual cannot be identified): ● Ethnicity ● Age range	This will help us answer questions about our membership demographic, and work towards addressing issues in access to services for people who may be marginalised

We will take the following measures to ensure that information is kept up to date and accurate:

- Monthly: a footer on our newsletter, reminding people how they can withdraw their information from SCCS' database
- 10 Yearly: a full review of all members, by email, offering to take them off the database if they respond with that instruction

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

Data Security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Using lockable cupboards (restricted access to keys)
- Password protection on personal information files, such as HR files
- Not allowing individuals' personal data to be taken off site (as hard copy, on a memory stick. NB homeworkers do use laptops, but these are password protected with encrypted folders for personal information)
- Back up of data to a hard drive which is kept in a locked cupboard
- Individuals' details will be available to two staff members only, and will kept on encrypted laptops
- Staff information will be kept in a specific HR folder, which is encrypted
- Hard copies of people's names and addresses will not leave the office / home office used by staff and freelance staff

All information will be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the rights of the individuals whose data is being processed
- Secure
- Not transferred outside the EEU without adequate permission

The Board and Trustees are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach that they have made.

Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

Any unauthorised disclosure of personal data to a third party by an employee may result in Disciplinary Action.

Information Security in Shared Office Space and mobile working

Information security applies to data which is electronically stored, electronically transmitted, printed, written or spoken. Whilst working in the hub, at the Alliance office in Glasgow, employed staff, freelance staff, trustees and volunteers must not discuss sensitive or confidential issues in the open plan area of the office. Documents relating to SCCS should not be left stored on the Hub PC as anyone working in the Hub can access the folders and these could be deleted or moved in error. Printed information must not be left lying at the printer and anything with sensitive or confidential information must be printed from the SCCS printer. Devices should be locked or logged off whilst not being used or the hub user is away from the hub desk.

Whilst working from home or in public places employed staff, trustees and volunteers must be careful about the information they are accessing, who can read it and who could overhear them.

Subject Access Requests

- Anyone whose personal information we process has the right to know:
- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong. Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to Eileen Moulton: info@skinconditionscampaignscotland.org

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- Their relationship with the organisation (e.g. former / current member of staff, trustee or other volunteer)
- Any other information relevant e.g. timescales involved
- Type of ID required before releasing any information e.g. passport, driving licence, birth certificate AND one current bill with the person's address

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within one month required by the new regulations coming in May 2018 from receiving the written request.

Review

This policy will be reviewed at intervals of 3 years, to ensure it remains up to date and compliant with the law. The current policy is an interim policy, due to be updated in line with changes in the law, in October 2016.

Declaration

I confirm I have read and understood SCCS's Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a Member of Staff / Volunteer / Trustee (delete as appropriate)

Signature:

Print name:

Date:

Please return this form to Eileen Moulton, SCCS.

For Internal Use Only

Data Protection Policy created on: 27.6.16

Created by: Jennifer Hill / Eileen Moulton

Approved by:

Review required on:

Reviewed by:

Reviewed on: