INTRODUCTION FOR NEW TRUSTEES

TRUSTEES' POWERS
Regulation
Our Constitution
Collective Responsibility
Sub Committees
Payment of Trustees

DECISION MAKING, RISK & CONTROL

BOARD EFFECTIVENESS

OFFICE BEARERS
Chair & Vice-Chair
Treasurer
General Secretary

VOLUNTEERS

CONTRACTORS

STAFF

DATA PROTECTION

APPENDICES

INTRODUCTION FOR NEW TRUSTEES

WELCOME! Congratulations & Well Done!

You may be asking yourself what have I agreed to? What does a Trustee do and what can't they do? What about the responsibility thing? What is this 'Corporate Governance' stuff you seem to hear more and more about? This guidance pack should be able to answer your questions.

'Corporate Governance' is a term used to describe how an organisation is organised and managed. It is a system which is designed to protect Trustees, members and other stakeholders. It is all straightforward with an obligation to do the right thing. If you are reading about it for the first time, read this whole document through including any links to supplementary information and guidance and reflect on what it says. It is designed to make the running of the SBA a well organised and transparent operation which offers protection to Trustees, using good practice and makes us an effective organisation and a credible one to our members, regulators and other outsiders.

The SBA was founded in 1912. It operated for a hundred years or so as an association, was first registered as a charity in 1942 and in 2015 transferred its operations into a SCIO – a Scottish Charitable Incorporated Organisation. SCIOs are designed to give some legal protection to charity trustees and to ensure that they operate with an acceptable level of corporate governance. They are regulated by the Office of the Scottish Charity Regulator – OSCR. We are accountable to OSCR and make regular returns to them.

A good place to start to understand more on what it means to be a Trustee of a Scottish Charity is the OSCR website where advice is available and downloadable in a few formats: -
https://www.oscr.org.uk/guidance-and-forms/guidance-and-good-practice-for-charity-trustees/
https://www.oscr.org.uk/news/an-easy-read-guide-to-being-a-charity-trustee/

Our official Scottish Charity Name and number are: -

Scottish Beekeepers Association (SCIO), SC009345

Registered charity from 14 October 1942

The SBA's constitution lays out the **policy objectives of the association** as follows. Trustees are expected to know the SBA's policy objectives and to promote them at every opportunity.

4 The organisation's purposes are to **support honeybees and beekeepers**, **improve the standard of beekeeping**, and to **promote honeybee products** in Scotland through:

4.1 The advancement of **education** in relation to the craft of beekeeping;
4.2 The advancement of the **heritage, culture and science** of beekeeping; and
4.3 The advancement of **environmental protection** by conservation of the honeybee.

All Trustees are expected to comply with the SBA's Trustees Code of Conduct (**App I**)

TRUSTEES' POWERS

Trustees have collective responsibility and are there to lead, control and supervise the SBA's activities. It is the part of the organisation with formal powers and responsibilities, which are detailed in our constitution and backed up by law.

If things go wrong, it's the trustees that will be called to account. They need to be aware of this and act in the best interests of the organisation and its beneficiaries, following all requirements of law and regulation. This is sometimes referred to as the need for 'due diligence'.

To enable the organisation to meet its aims, Trustees should perform the following functions:

- Set and maintain the vision, mission and values of the organisation.
- Develop direction, strategy and planning.
- Ensure the organisation has the appropriate structure and resources for its work.
- Establish policies and procedures to govern organisational activity, including guidance for the Board, volunteers and staff.
- Establish systems for reporting and monitoring, including to its members.
- Manage risk and ensure compliance and accountability with the constitution, OSCR and the law.
- Ensure that the financial affairs of the organisation are conducted properly.

Regulation

It's the responsibility of all Trustees to ensure that the SBA fulfils its obligations to OSCR. The charity should have procedures setting out who will do this. Failure to comply with regulatory requirements can have serious consequences.

On becoming a Trustee all Trustees are expected to complete a number of declarations which are designed to ensure that they are a 'fit and proper person' to hold such an office. These are part of the **Charities and Trustee Investment (Scotland) Act 2005** which outlines the legal duties charities and their trustees are obligated under. These include:

- Trustees' code of conduct
- Trustees' declaration of interest
- Section 69 declaration
- Section 70 declaration
- Section 66 declaration

A Tailored OSCR Charity Information and Guidance Pack for the SBA is produced annually and is available from the Treasurer or General Secretary.

Trustees should also be aware of the SBA's safeguarding policy. (**APP II**)

Our Constitution

All Trustees should be familiar with the SBA's constitution. It is our 'user manual' and sets clear boundaries on our activities. The most current and approved version is available on the SBA website

https://scottishbeekeepers.org.uk/about

The constitution should be reviewed by the Trustees periodically, paying special attention to the part setting out the purpose of the organisation. If this no longer reflects our circumstances and aspirations, it will be time to update it.

The constitution should lay out clearly the main policy objectives of the SBA. Care needs to be taken that over-prescriptive procedures are not written into the constitution. The normal place for detailed procedures would be in a supporting document which is given authority from the constitution, and which can be updated either by the Trustees or the members in general meeting.

Any organisation which becomes hidebound by procedure and forgets its original purpose has but a short time to live….

Wider approval from members, and in some cases, OSCR, may be necessary before aspects of the constitution can be changed. The consent of OSCR is required before we can alter any of our purposes as this could affect our charitable status. Trustees should regularly assess the risks associated with the organisation's current and planned activities and decide whether its legal status is still appropriate.

Collective Responsibility

All Trustees collectively have the ultimate responsibility for running a voluntary organisation, for its property, finances, staff and volunteers.

Trustees can delegate some of their authority (e.g. to staff, officials or sub-committees) but they can never delegate their responsibility.

As responsibility is collective, if there are any legal or financial repercussions from decisions made by the Trustees, then all members of that group are legally liable in equal proportion. The behaviour (or misbehaviour) of one Trustee is the concern of all. Similar support from all for an area of one Trustees officiant office of accountability is required, this includes understanding what is presented and actively contributing and not being passive.

If a Trustee is absent from a meeting, they are still responsible for decisions made when they were not present. Their absence does not absolve them from responsibility or liability.

The SBA has taken out Trustees Indemnity Insurance which protects Trustees *provided they have acted honestly and in good faith.*

Sub Committees

Sub Committees operate under the delegated authority of the main Board. All sub committees should have clear terms of reference and lines of reporting to the main Board.

If a sub committee has a budget (under the control of a designated budget holder who must be a Trustee) it must operate within the terms of that budget or seek further spending powers from the accountable Trustee or the Board. Any sub committee in this position should, in the first instance, consult with the Treasurer. Any declaration of personal interest which may be a conflict in a proposed project or activity must be declared.

A list of the approved SBA sub committees is contained in **APP III**.

Payment of Trustees

Trustees are generally unpaid. Third sector organisations are established for public benefit, and not for personal gain. A common exception is where a Trustee may be the best person to do a specific piece of work for the organisation, which would in any event be purchased. They may then be paid a one-off fee. Good practice dictates that Trustees should not receive any routine remuneration for their time or effort, though of course reasonable out-of-pocket expenses can be claimed subject to being properly authorised and have been included in the budget. Trustees who embark on an unbudgeted project on their own initiative should not expect to have any related costs reimbursed. If in doubt – consult with the Treasurer. For Scottish charities, payment of Trustees is allowed under certain conditions, including:

- the maximum level of payment is written down and agreed
- that this level is reasonable and, in the charity's, best interests
- that the charity's governing document allows such payment
- that only a minority of the Trustees receive such payment or are connected with trustees who do.

This would allow employees to join the Board of a charity but is not recommended as it can generate potential for conflicts of interest (the employee would theoretically also be their own employer)

DECISION MAKING, RISK & CONTROL

While the Board is ultimately responsible for the decisions and actions of the charity, the Board cannot and should not do everything. The Board needs to decide which matters it will make decisions on and those which it can and will delegate.

"Trustees delegate authority, but not responsibility, so the Board needs to implement suitable controls to make sure it oversees delegated matters."

Trustees must also **identify, assess and agree how to mitigate risks** and opportunities for the Charity and decide how best to deal with them including whether they are manageable or worth taking.

The Board should be clear that **its primary role is strategic, rather than operational** and reflects this in the matters it delegates. However, it is recognised that some Trustees are Office Bearers which require operational activity, in some instance operation tasks may be delegated via agreements with paid activity via Contractors or Employees.

The Board should put in place a sound decision-making framework that outlines

- its sub committees have suitable terms of reference, which are available to the Board
- the members of sub committees have appropriate skills and understand their accountability and boundaries in terms of freedom to act, or when they must defer to the Board
- the terms of reference are reviewed regularly and approved by the Board
- the sub committee membership is refreshed regularly and endeavours not to rely too much on particular individuals and ensures no conflict of interest.

The Board **regularly reviews what matters are reserved to the Board** and which can be delegated. **It understands and collectively exercises the powers of delegation** to office bearers, sub committees, individual trustees, staff or volunteers. These matters are documented in the terms of reference and are agreed by the Board, which gives enough detail and clear boundaries so the delegations can be clearly understood and carried out.

The Board identifies its information needs and receives associated performance information, which is timely, relevant, accurate and in an easy to understand format.

The Board retains overall responsibility for risk management and discusses and decides the level of risk it is prepared to tolerate. The Board promotes a culture of prudence with resources but also understands that being overcautious and risk averse is itself a risk.

BOARD EFFECTIVENESS

The Board works as an effective team using the appropriate balance of skills, experience, characteristics and knowledge to make informed decisions. The tone the Board sets through its leadership, behaviour and culture, and its overall performance is central to the success of the charity. Trustee recruitment, performance and development should therefore be treated with a similar professional approach to that of executive recruitment and retention in public and private organisations. Trustees need to ensure that Trustee appointment identifies suitable skills in a wider

aspect of being on a Charity Board as well as any specific beneficial knowledge, qualification, skill or lived experience. The following should be observed: -

- The Board meets as often as it needs to be effective.
- Meetings have a well-structured agenda and are well chaired.
- Trustees are provided with timely and clear information so that they come to meetings prepared.
- The Board has a vice-chair, 'senior independent trustee' or similar, who provides a sounding Board for the chair and serves as an intermediary for the other trustees if needed. This person may be a deputy or vice-chair or vice-president of the charity.
- The Board, **collectively**, can get access to independent professional advice at the charity's expense if this advice is needed for the Board to discharge its responsibilities.

The Board has, and regularly considers, the skills, knowledge and experience it needs to govern, lead and deliver the charity's purposes effectively. It reflects this mix in its Trustee appointments.

When considering this, the Board and the Chair in particular, will have reference to the individual characteristics of the Trustees so that that the Board can act as a balanced unit, with Board development being identified and taking place from time to time as needed. Other Trustees in the Board may be identified to lead this where skill, knowledge or lived experience applies.

OSCR produces guidance on 'Taking Steps to Successful Trustee Recruitment which is available

https://www.oscr.org.uk/guidance-and-forms/managing-a-charity-guidance/taking-steps-to-successful-trustee-recruitment/

OFFICE BEARERS

Chair (President)

The Chair (President) has an important leadership role in guiding the SBA and ensuring that it operates effectively, and acts as its external face to the outside world and will represent the organisation at external events and meetings. The Chair, working with the Board, is responsible for leading the governance of the organisation and ensuring its effectiveness.

It is the responsibility of the Chair (President) to identify and recruit, as far as is practically possible, new Trustees with the appropriate professional and personal skills, and to ensure a Board with a range of diversity and equality in keeping with current legislation. Key duties can include:

- Ensuring governance procedures are reviewed at appropriate intervals
- Taking a strategic view of the issues facing the SBA and guiding the Board accordingly
- Preparing agendas for the meeting in consultation with the General Secretary and other Trustees
- Ensuring meetings are run efficiently, and discussion and decision-making is democratic and fully participative
- Ensuring that specialist sessions are chaired by the most appropriate Trustee – generally the Trustee who has specialist knowledge of a particular topic.

- Where meetings last more than three hours, ensuring that the chair rotates – to the Vice-Chair or other competent Trustee - to ensure that the discussion (and Trustees) stay fresh and alert.
- Holding the casting vote in the event of a split decision
- Ensuring that AGMs and EGMs are carried out in accordance with the constitution.

Vice- Chair (Vice President)

Many organisations also appoint a Vice-Chair (Vice President) to share the workload and deputise for the Chair in activities as outlined above. The Vice-chair is an office in its own right. Frequently, the Vice Chair will in due course or in the case of contingency, step up to become Chair.

Treasurer

It is important that all Trustees collectively play their part in financial monitoring and decision making. The Treasurer's primary role is to assist and advise the Board in overseeing the finances even if paid employees or contracted services deal with much of the day-to-day financial business. Some of the tasks can include: -

- Controlling and accounting for the organisation's finances
- Setting Financial Controls and delegation of authority for financial activities and budgets
- Being a counter signatory to any major banking transaction
- Overseeing bookkeeping
- Presenting financial reports, including the annual accounts at the AGM and raising issues and answering questions at Trustee meetings and AGM
- Liaising with the auditors or financial examiners for the annual review of accounts
- Ensuring statutory financial returns are made to OSCR (The Treasurer is the designated Principle Contact for OSCR)

The Treasurer controls the SBA's finances on behalf of the Board. The Treasurer achieves this by

- Overseeing the recording and monitoring of the financial transactions
- Preparing an annual budget in conjunction with the budget holders and reporting against this
- Advising the Board on financial matters
- Overseeing the preparation of annual accounts
- Making statutory returns to OSCR

The Treasurer should always be consulted on any commercial agreement, be a signatory and may be designated as the Trustee responsible for holding relevant Contracts, in agreement with the SBA official Office Bearers (President, Vice President, General Secretary & Treasurer).

General Secretary

The Secretary is responsible for many specific tasks, some of which will be regular practical administrative duties of paid staff in larger organisations. This includes:

- Legal contact for the organisation
- Managing the day to day contacts with the organisation and either responding directly or in conjunction with the relevant Trustee
- Acting as the principal point of contact with secretaries of ABAs
- Convening meetings and booking rooms
- Dealing with correspondence
- Preparing agendas for meetings (in consultation with the Chair)
- Taking the minutes of meetings and ensuring back-up information is available where required
- Maintaining a database of SBA policies and procedures and all formal Charity Board documentation, such as minutes of formal meetings.

Unless our constitution states it as a requirement (it doesn't), we no longer need to have to have a Company Secretary under company law. The position of a 'Company Secretary' has a specific legal meaning and is responsible for ensuring that regulations are complied with.

The General Secretary maintains the statutory records of the SBA (such as the register of Trustees) on behalf of the Board and any other documents that need to be regularly signed by Trustees, Sub Committees etc, such as Information Security and Data Processing.

Should the organisation employ any staff, the General Secretary will be responsible for ensuring employment contracts are appropriate and legal, they will also be the custodian for any such contracts.

STAFF, CONTRACTORS AND VOLUNTEERS

The Trustees have responsibility for the overall governance and direction of the organisation and have a duty of care for volunteers and staff.

It is important to be clear about separate roles and responsibilities and legal liabilities. There should be policies and procedures on delegated decision-making and tasks. Some tasks should never be delegated to staff or non-office bearing volunteers, e.g: recruitment, support, supervision and appraisal of senior employees, final decisions on key staffing issues such as disciplinary and grievance procedures.

Trustees have key legal obligations including:

- Ensuring employees receive written terms of employment
- Consulting with employees regarding redundancies, mergers and health and safety
- Employee liability insurance

AT the time of this version of this document there are no employees of the organisation and this guidance may need updated in the event this changes.

Where is exists, the lines between governance and management can be blurred, particularly where duties are carried out by volunteers. The broad difference is that governance is about strategy and management is about operations. However, some Trustees may be directly involved in operations due to offices or remits they are assigned. Approach must be sensible, and Sub Committees and their Terms of Reference are important to make clear what is within the gift of that sub Committee to decide and act on and what needs to be deferred to the Board.

Governance	**Management**
Overview of the organisation as a whole	Day to day operation of activities or projects
Long term direction	Short to medium implementation of plans
Processes and framework for effective working	Detailed planning and supervision
Accountable for actions and decisions	Responsible for delivery

DATA PROTECTION & INFORMATION GOVERNANCE

Any organisation which holds and processes information about its members, clients, employees or suppliers, is legally obliged to protect that information.

Under the Data Protection Act an organisation must:

- Only collect information that is needed for a specific purpose (relating to the organisation's purpose)
- Keep it secure (physical and digital)
- Ensure it is relevant and up to date
- Only hold as much as it needs, and only for as long as it needs it (advice on retention dates are available)
- Allow the subject of the information to see it on request

An organisation which handles personal information may need to register with the Information Commissioner's Office (ICO) as a data controller. Notification is a statutory requirement and every organisation that processes personal information must notify the ICO unless they are exempt. Failure to notify is a criminal offence. Links to understand more about the ICO and our obligations are: -

https://ico.org.uk/for-organisations/
https://ico.org.uk/for-organisations/in-your-sector/charity/charities-faqs/

Currently, the SBA is not registered with the ICO as it is considered that registration is not necessary as we are exempt, which was re-established in Feb 2020 via the following assessment: -

https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/y/N/Y/Yes

The SBA holds information on:

- Its membership
- Trustees
- Suppliers

Therefore, the ICO deems that we are exempt as SBA :

- only process information necessary to establish or maintain membership or support
- only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
- you only hold information about individuals whose data you need to process for this exempt purpose
- the personal data you process is restricted to personal information that is necessary for this exempt purpose

SBA processes comply with the General Data Protection Regulation (GDPR) as it has an Information Security Policy that requires **all** Trustees, Sub Committee Members, official Volunteers, Consultant and Contractors to the organisation to sign its appendix A and also complete B and C where relevant. The current version of that document is V6 May 2019 and will be reviewed regularly. **See App IV**

The Scottish Beekeepers' Association

Trustees' Code of Conduct

Note: this document contains 2 pages

Introduction

The purpose of this code of conduct is to provide trustees with clear guidelines as to their standard of behaviour, responsibilities, and best practice in fulfilling their obligations to The Scottish Beekeepers' Association (SCIO)(the SBA).

This document should be read in conjunction with the trustee role descriptions and the constitution, prior to completing the charity's declaration of interests form.

General

1 Trustees should familiarise themselves with the seven Nolan Principles of Public Life (selflessness, integrity, objectivity, accountability, openness, honesty and leadership), and act in accordance with them.

2 Trustees must have a good understanding of, and be sympathetic with, the aims and objects of the SBA and act in accordance with the constitution at all times.

3 Trustees must act and make decisions in the best interests of the SBA and its present and future beneficiaries.

4 Trustees should do their best to avoid conflicts of interest and complete the trustees' declaration of interests form. Where they do find themselves in conflict, trustees should declare that fact and not take part in any relevant decision making, in accordance with the constitution.

5 Where assistance and advice is required for the trustees to be able to make the most appropriate decision affecting the SBA, that assistance/advice should be sought from an appropriate source (e.g. Charity Commission, or professional adviser) and considered carefully.

6 Trustees must play an active role in trustee Board meetings, having spent due time preparing and reading Board papers in preparation for meetings. A regular attendance at meetings is required of trustees to ensure that best practice in governance is reached and maintained, in accordance with the requirements in the constitution.

7 Trustees must not receive any financial or non-financial benefit that is not explicitly authorised by the governing document or the Charity Commission. Trustees should not exert any influence to garner any preferential treatment for themselves or their family, or other connected persons.

8 Trustees are jointly and severally liable for their decisions, therefore decisions should be taken together, as a team, recorded accurately in the minutes, and communicated to members, staff, beneficiaries and funders in a unified manner.

9 Trustees are accountable to a range of interested parties for their actions and as such, decision- making and governance issues should be as transparent as possible, except when confidentiality is required.

10 Should a trustee feel they require further guidance or training in their role, it is their responsibility to inform the General Secretary, and in liaison with the General Secretary to develop opportunities for training on an individual or group basis.

11 Any information of a confidential nature must remain so outside the confines of the trustee meeting.

12 Trustees must sign any declarations required by OSCR and HMRC.

Version 3.0a, August 2014

The Scottish Beekeepers' Association

The Scottish Beekeepers Association is a Scottish Charitable Incorporated Organisation, registered in Scotland, number SC009345.

Safeguarding Policy and Guidelines

Note: this document contains two pages

Introduction

This safeguarding policy provides a policy statement and guidelines for all members, covering the activities and events that take place within the Scottish Beekeepers' Association (SCIO) (the SBA).

Policy Statement

It is the policy of the SBA to make every effort to safeguard its members from physical, sexual and emotional harm while participating in association events and activities. The SBA takes all reasonable steps to ensure that, through relevant procedures and training, children, young people and adults taking part in SBA events and activities do so in a safe environment.

Guidelines

All members, in whatever capacity they are carrying out SBA activities, have an obligation to avoid creating distressing situations between themselves and others with whom they come into contact in the course of their SBA activities. This obligation covers activities involving adults, and young people of any age. The trust required between SBA members or volunteers and participants is fundamental to the SBA's undertakings, and therefore should not be jeopardised. For this reason all SBA members working with others in the course of volunteering or carrying out their designated SBA responsibilities must follow these guidelines.

Code of conduct

As an SBA member, volunteer or trustee you are expected to:

- · respect everyone as an individual
- · provide a good example of acceptable behaviour
- · respect everyone's right to privacy
- · show understanding when dealing with sensitive issues

- · adhere to the SBA's safeguarding policy statement and guidelines

As an SBA member, volunteer or trustee you may not:

1. · permit abusive behaviour
2. · have inappropriate physical or verbal contact with others
3. · jump to conclusions or make assumptions about others without checking facts
4. · encourage inappropriate attention-seeking behaviour
5. · show favouritism to anyone
6. . make suggestive or inappropriate remarks or actions deliberately place yourself or others in a compromising situation

Other adults present

Members, volunteers and trustees should avoid situations where they are alone with a young person under the age of 18, or a vulnerable adult. Ideally, the third person present should be an adult who knows the person concerned. This precaution protects all parties by removing a potential/any feeling of threat by an insecure participant, and by providing a witness if an accusation of improper behaviour is made.

Physical contact

Physical contact between an individual and the member, volunteer or trustee should be avoided. There are instances when it is necessary, e.g. to demonstrate a skill or activity, but such contact should remain impersonal so there is no risk of it being misinterpreted.

Appropriate language

Care should be taken about what is said, and the way it is said. Members, volunteers and trustees should avoid saying anything which could be interpreted as being aggressive, suggestive, or containing an innuendo.

Favouritism

Members, volunteers and trustees should avoid showing favouritism. There are times when people find it easier to relate to one person. However, singling them out can create a feeling of resentment from others in the group or organisation, or they can become the object of personal attack from others. Similarly, unrealistic expectations can be created, and the motive misunderstood.

Creating impressions

It is important that members, volunteers and trustees do not create a false impression. Words and actions can be misunderstood, and care should be taken to avoid awkward situations. Should such a situation arise, it is essential to handle it with care and consideration to minimise embarrassment to all involved.

Support for members, volunteers and trustees

The SBA endeavours to co-operate fully with any external organisations which have a concern for the safety of vulnerable people in society at risk from inappropriate behaviour and attitudes.

If you have any concern about a member of the SBA of someone involved in an SBA activity or event, please contact the President or another trustee.

PVG (Protecting Vulnerable Adults)

The SBA will require those trustees, officers and those formally contracted with the SBA with particular responsibilities which involves working in an unsupervised capacity with children under 18 to be registered under the Government's Protecting Vulnerable Adults Scheme. The secretary of the SBA will administer the scheme for the SBA. The SBA will operate the PVG scheme for all those Affiliated Beekeeping Organisations in Scotland that request it. The SBA will encourage at least one member in each ABA to be registered with the scheme.

Version 1 August 2017

APP III – SUB COMMITTEES

Office	Officer	Sub-Committee	Area of activity
Secretary	Helen Nelson	Not currently	Official legal contact point for the SBA. – Manages the mailbox. Distributes queries to relevant Officers.
Treasury	Helena Jackson	Not currently	All things financial
Development	Michelle Berry	Not currently but reports to Alan R.	Development of the SBA to increase its recognition as Scotland's leading bee charity & to identify methods of achieving this.
Bee Health	Gavin Ramsay	Not currently	All health & medicines + contact with Scottish Government (SG) Bee Health Group
Science	Gavin Ramsay	Not currently	Any contacts from researchers & anyone wishing to share bee science stuff
Shows & Publicity	Enid Brown	Informal group formed around Highland show Enid, Bron, Alan R, Janice Furness, Phil McA, Susan Fotheringham, Cynthia Riach, Pete & Christine Matthews. Mtgs chaired by Enid Brown and minutes by AR	Show attendances, honey shows
Promotion of Beekeeping	Alan Riach	No official sub-committee but works through above show group & interacts with Publicity function of	Very closely tied to shows, so work closely with Enid and Michelle

		Shows + activities of Development Officer	
Education	Alan Riach	Alan R (Trustee), Bryce Reynard, David Wright (Members)	All exam and workshop stuff & guidance on Tour Speaker & Autumn Convention
Moir Library	David Wright	Bron Wright, Alan R (Trustees) David Wright, Nigora Asaeva, Margaret Forrest, Nigel Hurst (Members)	Promotion & maintenance of the Moir and use of its facilities.
Information, Communications & Technology (ICT)	Julian Stanley	Julian, Alan R, (Trustees) + Kevin Russell (webmaster) Chris Urie & Michelle Berry	Development & maintenance of all ICT activities including Website, & social media sites
SBAi Forum	Gavin	Gavin (Trustee)+ David Evans (Moderators)	Maintenance of interactive forum.
Membership	Mhairi Neill	None	Control of membership
Insurance & Loss Compensation	Alan Mackie is the non-trustee Advisor	None - liaises with Phil McA	Negotiation of Insurance & settlement of Compensation claims
Markets	Margaret Thomas	None currently	Advice on market regulation and prices
Autumn Convention	Does not have an officer, Board appoints a temporary officer to run it		
Area Reps	East – David Macadam, North East – Andy Watson	Area Reps liase with one another They are elected by the Affiliated Beekeeping	Liaison between the SBA & the ABA's via the ABA Representative Person (usually the ABA Secretary)

	North- Vacant North West – Vacant West – vacant	Association (ABA) groupings in their area and then accepted by the SBA Trustee Board as Trustees for their period of office.	

Information Security Policy

The Scottish Beekeepers' Association (SCIO)

Registered Charity No. SC009345

May 2019

Contents

1. Introduction 22
2. Information Security Policy 22
3. Acceptable Use Policy 23
4. Disciplinary Action 23
5. Protect Stored Data 23
6. Information Classification 24
7. Access to the sensitive cardholder data 24
8. Physical Security 24
9. Protect Data in Transit 25
10. Disposal of Stored Data 26
11. Security Awareness and Procedures 26
12. Incident Response Plan 27
13. Third party access to card holder data 29
14. User Access Management 29

Appendix A 30

Appendix B 31

Appendix C 32

1. Introduction

This Policy Document encompasses all aspects of security surrounding personal and confidential information used and retained within the Scottish Beekeepers' Association (the organisation) and must be distributed to all Trustees, Authorised Officers, Sub-Committee Members, Volunteers, Consultants and Contractors to the organisation, including any Volunteers who may receive or handle information. All those issued this document must read it in its entirety and sign the form confirming they have read and understand this policy fully and the implications in relation to their access and use of information provided to the organisation. This document will be reviewed and updated by the Trustees on an annual basis or when relevant and distribute it as applicable.

2. Information Security Policy

The Scottish Beekeepers' Association handles personal and potentially confidential or sensitive information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Personal data is described along with other key definitions by the Information Commissioner Office and we request that you familiarise and keep yourself informed on these via the ICO website

https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees

The Scottish Beekeepers' Association commits to respecting the privacy of all its members, volunteers and customers and to protecting any data about them from outside parties. To this end Trustees are proactively working to providing and maintaining secure environments in which to process information so that we can meet these commitments.

Trustees, volunteers or anyone acting on behalf of the organisation may be required to handle confidential information. Confidential information includes but is not limited to personal information, and organisation data. Trustees, volunteers and anyone acting on behalf of the organisation should ensure they:

- Handle personal and confidential information in a manner that fits with their sensitivity;
- Do not disclose personal and confidential information unless authorised;
- Protect personal and confidential information;
- Keep passwords and accounts used for the purposes of the organisation in a secure manner;
- Request approval from The Trustees, one of which must be the IT Trustee prior to establishing any new software or hardware, third party connections, etc. ensuring appropriate security and information management policies are contracted;
- Do not install unauthorised software or hardware that will hold or process personal or confidential information provided to the organisation by its members, volunteers or cardholders, unless you have explicit Trustee approval;
- Always leave desks clear of personal and confidential information related to the organisation and its members and lock computer screens used for processing when unattended;
- Information security incidents must be reported, without delay, to the Trustee responsible for incident response locally – if in doubt this should be reported to General Secretary and President.
- Do not use e-mail, internet and other organisations' resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;

- We each have a responsibility for ensuring our organisation's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the detail herein you should seek advice and guidance from the Trustee aligned to area of activity related.

3. Acceptable Use Policy

The Trustees' intentions for publishing an Information Security Policy are not to impose restrictions that are contrary to the Scottish Beekeepers' Association established culture of openness, trust and integrity. Trustees are committed to protecting the Trustees, Volunteers, Contractors, and the organisation from illegal or damaging actions by individuals, either knowingly or unknowingly. The Scottish Beekeepers' Association will maintain an approved list of technologies and individuals (Trustees, Authorised Officers, Sub-Committee Members, Volunteers, Contractors) with access to such devices as detailed in Appendix B.

- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors are responsible for exercising good judgment regarding the reasonableness of accessing and using personal or confidential information.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should ensure that they have appropriate knowledge and are authenticated for the use of technologies.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should take all necessary steps to prevent unauthorised access to personal and confidential information.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should ensure any related passwords are kept securely and do not share accounts, unless in exceptional and documented circumstances.
- Authorised users are responsible for the security of their passwords and accounts.
- All electronic devices, inclusive of PC's Laptops, mobile phones and portable storage devices used for the access and or processing of the organisations personal or confidential information should be secured with a password-protected screensaver with an automatic activation feature.
- All POS and PIN entry devices should be appropriately secured so they cannot be tampered with or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised whilst in transit.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors must use extreme caution when opening organisation related e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. Anything of suspicion should be investigated locally and deleted and not forwarded on to other organisations authorised users.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by Trustees and authorised Officers and Volunteers will result in action, from warnings, to removal of position and possible membership (in line with the Scottish Beekeepers' Association Constitution). Claims of ignorance, good intentions or using poor judgment will not be acceptable as excuses for non-compliance.

5. Protect Stored Data

All data stored and handled by Trustees, Authorised Officers, Sub-Committee Members, Volunteers and

Contractors must always be securely protected against unauthorised use. Any personal or confidential data that is no longer required by the organisation for business reasons must be discarded in a secure and irrecoverable manner.

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block for payment cards under any circumstance.

6. Information Classification

Data and media containing data should always be labelled to indicate sensitivity level

- **Confidential data** might include elements of personal data and or information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the organisation if disclosed or modified. **Confidential data includes payment or cardholder data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorised disclosure, sensitive to the running or objectives of the organisation;
- **Public data** is information that may be freely disseminated.

7. Access to the sensitive cardholder data

All Access to sensitive cardholder data should be controlled and authorised. Any functions that require access to cardholder data should be clearly defined.

- Any display of the card holder data should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as Permanent and or Primary Account Number(s) (PAN's), personal information and business data is restricted to Trustees and authorised Officers and Volunteers that have a legitimate need to view such information, these individuals should complete the form listed in Appendix A
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
- The organisation will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the cardholder data that the Service Provider possess.
    - The organisation will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
    - The organisation will monitor the Payment Card Industry Data Security Standard (PCI DSS) compliance status of any listed Service providers, via the annual production of their Compliance Certificate, which will be issued to the Treasurer.

8. Physical Security

Access to personal and confidential information in both hard and soft media format must be physically

restricted to prevent unauthorised individuals from obtaining such information.

- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors are responsible for exercising good judgment regarding the reasonableness of confidential data. If in any doubt, do not proceed.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should take all necessary steps to prevent unauthorised access to Confidential and internal use data which includes card holder data.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should ensure that technologies should be used and setup in acceptable locations, that are secure and not in an open public space with a potential for theft or inappropriate observation of data being accessed.
- A list of devices that accept payment card data should be maintained (Appendix B).
- The list should include make, model and location of the device, the serial number or a unique identifier of the device and be updated when devices are added, removed or relocated
- Point of Sale (POS) devices surfaces should be periodically inspected to detect tampering or substitution.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors using the devices should be trained and aware of possible security issues whilst handling the POS devices
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors using the devices should verify the identity of any third-party personnel claiming to repair or run maintenance tasks, install new devices or replace devices.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the Shows and Publicity Officer.
- Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals. (Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.)
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered with or altered.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and must be approved by the Trustees.
- All computers that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

9. Protect Data in Transit

All Personal, Confidential or internal use data must be protected securely if it is to be transported physically or electronically.

- Confidential or internal use data should never be sent over the internet via instant chat or social media unless you have direct consent to do so from all individuals involved. Personal or Confidential Data that is transmitted via email should be limited and where possible via files that have encryption applied, where possible.
- If there is a business justification to send Confidential or internal use data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc).

- The transportation of media containing Personal, Confidential or Internal Use data to another location must be authorised by the relevant Trustee, and logged before transportation. Only secure courier services may be used for the transportation of such media. The status of the shipment should be recordable and monitored until it has been delivered to its new location and signed for.

10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by the organisation, regardless of the media or application type on which it is stored.
- A process must exist to permanently delete any electronically held data, when no longer required.
- All hard copies of Personal, Confidential or Internal Use data must be manually destroyed as and when no longer required for valid and justified business reasons (i.e. once transactions have been confirmed as successful). A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- The organisation will identify the process for the destruction of hardcopy (paper) materials as part of Appendix C. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- The organisation will have documented procedures for the destruction of electronic media and requires:
    - All Personal, Confidential or internal use data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All Personal and Confidential information awaiting destruction must be held in lockable storage clearly marked “To Be Shredded/Incinerated” - access to these containers must be restricted.

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into organisational practice to maintain a high level of security awareness. The protection of Personal, Confidential or Internal use data requires regular instruction and or training of all Trustees, authorised Officers, identified Volunteers and contractors.

- Review handling procedures for sensitive information including use of POS devices and hold periodic security awareness meetings to incorporate these procedures into practice.
- Distribute this security policy document to all Trustees, authorised Officers, identified Volunteers and contractors to read. It is required that all Trustees, authorised Officers, identified Volunteers and contractors confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS) and present their compliance certificates annually.
- All third parties with access to Personal and or Confidential data are contractually obligated to comply with GDPR and annually provide evidence that they do so.
- This and any associated policies or procedures must be reviewed annually and updated as needed.
- Instruct, through this policy, that all Trustees and any identified Officers use a standard email Signatory (electronic) format which will include the following SBA Disclaimer statement: -

- The information contained within this e-mail and in any attachment is confidential and privileged. If you are not the intended recipient, please destroy this message, delete any copies held including any attachments and notify the sender immediately of the error. You should not retain, copy or use this e-mail for any purposes nor disclose any part of it to any other person other than the originator.

12. Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to communications or information including manual or electronic processing systems. If deliberate, the attacker could be a malicious stranger, or disgruntled Trustees, authorised Officers, identified Volunteers and contractors, and their intention might be to steal information or money, or just to damage our organisation. This also relates to accidental actions of any Trustees, authorised Officers, identified Volunteers and contractors, which involves sensitive data release inappropriately as guided by this policy.

Incident Response Notification

1. In the event of a suspected security breach, alert the relevant Trustee related to the area or function you are participating in.
2. The Trustee will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the Trustee will alert fellow Trustees and begin informing all relevant parties that may be affected by the compromise, including any commitment made in the organisation's Privacy Statement.
4. If the incident relates to cardholder details the following steps must be taken:

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.

Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs via 0800-89-1725

- 0800-89-1725.
- For more Information visit: https://www.visa.co.uk/contact-us.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
   a. Include overview of the incident
   b. Include RISK Level (High, Medium, Low)
   c. Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures
    a. Include forensic tools used during investigation
V. Findings
    a. Number of accounts at risk, identify those stores and compromised
    b. Type of account information at risk
        - Identify systems analysed if applicable. Include Domain Name System (DNS) names, Internet Protocol (IP) addresses, Operating System (OS) version, Function of system(s)
    c. Timeframe of compromise
    d. Any data exported by intruder
    e. Establish how and source of compromise
    f. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
    g. If applicable, review VisaNet endpoint security and determine risk
VI. Compromised Entity Action
VII. Recommendations
VIII. Contact(s) at entity and security assessor performing investigation

MasterCard Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
2. Distribute the account number data to its respective issuers.

American Express Steps

1. Within 24 hours of an account compromise event, notify American Express Merchant Services
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers
   Obtain additional specific requirements from American Express

13. Third party access to card holder data

- All third-party companies providing critical services which includes data hosting to the organisation must provide a contract which contains suitable evidence of relevant Data Security, such as in the form of an Information Asset Register and Privacy Statement or Security Policy.
- All third-party companies which have access to Card Holder information must:
  1. Adhere to the PCI DSS security requirements.
  2. Acknowledge their responsibility for securing the Card Holder data.
  3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
  4. Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.

14. User Access Management

- Access to Personal, Confidential or Internal Use data, including any data mentioned in the Scottish Beekeepers' Association Privacy Statement is controlled through the collation of Appendix C which is agreed by the Trustees and reviewed regularly.
- Each 'user' who may be Trustees, authorised Officers, identified Volunteers and contractors is identified along with the data they will be accessing for any purpose in the organisation's Information Asset Register (IAR) and will clearly identify who is accessing what sensitive data for what purpose, and the 'user' is made responsible for their actions. This is available in Appendix C.
- Access to all the organisation's information and data, including any in systems, can only be started after proper procedures are completed, the access recorded in the IAR, and this policy read, and a copy of Appendix A signed.
- As soon as an individual is no longer acting on behalf of the organisation, all his/her system logons must be immediately revoked, and any media returned or witnessed to be destroyed following the above clause.

Appendix A – Agreement to Comply Form – Agreement to Comply with Information Security Policy

_____

Name (printed)

I agree to take all reasonable precautions to assure that the organisation's internal information, or information that has been entrusted to the organisation by third parties such as members and customers, will not be disclosed to unauthorised persons. At the end of my tenure as trustee, or I no longer am a member of the organisation, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the relevant Trustee.

I have access to a copy of the Information Security Policy, I have read and understand this policy, and I understand how it impacts my role within the organisation. As a condition of continued tenure as a trustee or officer, I agree to abide by the policy and other requirements found in the organisation's information security policy. I understand that non-compliance will be cause for disciplinary action as per the organisation's Constitution, and perhaps criminal and/or civil penalties. I also agree to promptly report all violations or suspected violations of information security policies to the General Secretary.

_____

Signature

Appendix B – Electronic Devices – Used to Hold Personal or Sensitive Data

Asset/Device Name	Description	Owner/Approved User	Location

List of Service Providers (Contracted Services where relevant)

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant (if relevant) Including Date

Appendix C

GDPR Information Asset Register for

The Scottish Beekeepers' Association (SCIO) Registered Charity No. SC009345

Date completed/reviewed: 2019 (review)
Completed by: Trustee

Under the new principle of data accountability, organisations need to be able to demonstrate their compliance with the GDPR. This requires the organisation to maintain records of what personal data we hold, who has access to it and how it is securely stored. Completing this table is not a legal requirement but it is recommended to demonstrate good security procedures and designed to complement the SBA Information Security Policy.

Type of Personal, Confidential Information	Location of data	Who has access to the data and for what purpose*	Data retention period	Destruction Method
			.	

**The President, Vice President, General Secretary and Treasurer may not have regularly access to data listed for day to day organisational activities under their 'office'. However, should an incident arise where there needs to be an investigation for whatever reason, any of The President, Vice President, General Secretary and Treasurer will request access to any in*