SBBOT Governance - Policy – Data Protection

This statement of policies and procedures is based on:

- *The Observatory's existing Data Protection Policy, last approved September 2019*
- *Information taken from: 'General Data Protection Regulation: A Guide for Charities' produced by The Charities Finance Group (a group of 1400 charity finance professionals). The report is available on-line.*
- *Further information gained from 'Data Protection Policy,' an on-line document available for free download from www.donut.co.uk*
- *Conditions imposed by the General Data Protection Act which comes into force on May 24th 2018*

POLICY

A. The four main risks in data protection are:

- *breaches of confidentiality*. For example, by members' information being given out inappropriately to third parties or by our computer system being hacked.
- *Failure to offer choice*. For example, by members' not being given a say in *how* we approach them, what we approach them *for* and the *uses* to which we put any data that we hold on them.
- *reputational damage* to the Observatory by any publicised data breach.
- *Falling foul of the Information Commissioners Office* or the *Charities Commission* in the event of a serious data breach (see below).

B. General principles of data collection and processing under the new GDPR, as they apply to SBBOT:

1. SBBOT will only collect and hold data *lawfully, clearly and transparently*.
2. The *SBBOT Membership Form* is the basis of the Observatory's record of members' data, but we may also consult the Royal Mail and other databases to verify details of any postal addresses that members provide. We may also compile separate lists for other sub-groups, as listed below, under paragraph 3.
3. By 'data' we mean:
   - *membership details*
   - *volunteer details*, *including the Conservation Team*
   - *WEX and Phoenix details*
   - *ringers details*
   - *employees details*
   - *details of financial transactions and dealings with suppliers*, *including the suppliers' own details.*
4. We will only collect data for *specific identified purposes* and *not then use it for any other purpose.*
5. We will only collect data that is *adequate for the purpose and no more.*

6. We will only make use of *accurate and up-to-date data*.
7. There is a concomitant *responsibility for members* of the Observatory to inform the Trust of any changes in their own details.
8. Members' personal data will *not be used to record any aspect of their bank account* or other financial information, apart from a simple payment record.
9. We may use members data for *statistical analysis purposes*, but never in such a way that individuals could be identified
10. We will ensure that storage of data is *secure* and kept for *no longer than is necessary for the immediate purpose.*
11. Members have a *legal right to access any data* the Trust might hold about them.
12. We will *never sell personal data* to any third party.
13. All personal data will be accessible to the *smallest possible number of Trust personnel or members* that is compatible with efficient use of that data.

C. Trustees' responsibilities under GDPR:

1. Trustees are responsible for putting *policies and procedures* in place to ensure that the Observatory *follows data protection law,* which, effective from May 2018, will be the GDPR.
2. Under the terms of the GDPR, the Observatory Trust *as an organisation* legally becomes a '*Data Controller'*.
3. The Trust needs to be aware that any *serious* data breaches must be reported to the Charities Commission and the Information Commissioners Office which is the Regulator set up by the Government.

D. Other issues and comments:

1. The Trust does not use *third-party fund-raisers* so ensuring data protection in this area is not relevant to us**.**
2. The Trust does not pass on funds to any beneficiaries so is not concerned with '*Managing Data related to Beneficiaries'*).

Procedures

General and Membership-related

1. The only people at SBBOT able to access data will be *those who need it for their work at the Observatory.*
2. If they handle data, staff and volunteers will be *made aware of the processes and controls* which are in place to protect data and *their own responsibilities in this area*. Volunteers or other persons who do not routinely handle data, will *still be made aware of the general issues, policies and practices to protect data*. (For example, a shop volunteer must not pass on a member's contact information or other personal data without that member's permission).
3. Membership data will be primarily collected from the *membership form*, stored on a *secure computer* and *used for the following purposes*:
    - *administration of membership - names; postal addresses; e-mail addresses; telephone numbers and any other information (e.g. medical or personal data) that may have been voluntarily divulged.*
    - *administration of volunteer records*
    - *administration of donations, legacies and the 200 Club*
    - *distribution of Newsletters and Annual Reports*
    - *communications to members concerning their membership*
    - c*ommunications concerned with activities of the Trust*
    - *prevention and detection of crime*, *as required by law*

4. We will put well-publicised systems in place *for any member to exercise their legal right to find out what information is held about them* and for them *to be able to easily request changes or deletions*. Such requests must be made *in writing* (not e-mail or verbally) and addressed to the *Data Protection Officer* (see below) at the Observatory. The Trust will ensure that these changes are then made as soon as is possible.
5. All personal data will normally be accessible *only to the* Data Protection Officer and those deemed by him / her to have necessary need and then only when it is exclusively for the Trust's legitimate activities.
6. Although it is not a legal requirement, one Trustee will take on the role of *Data Protection Officer*, whose role will be to :
    - *keep Trustees updated* about their data protection responsibilities
    - *review all data protection policies and procedures*, in line with an agreed schedule
    - *arrange training, advice and guidance* for Trustees, employees and volunteers
    - *handle data protection enquiries* from within or outside of the Observatory
    - deal promptly with requests from individuals to see what data SBBOT holds about them (*'subject access requests'*)
    - *check and approve any contracts or agreements* with third parties which may handle the Trust's sensitive data.

Fund Raising:

1. *Donor consent will be obtained*. Generalised or implied consent for the Observatory to approach members is *no longer acceptable* and the Trust will implement '*explicit opt-in consent'*, effective from the date of ratification of this policy and procedures document.
2. The Trust will always be able to show *exactly why* it is collecting data for fund-raising
3. The Trust will not *store fund-raising data indefinitely*, without good reason or by permission of the members concerned.

4. Gift Aid declarations must *only be kept for 6 years*

Managing Financial Data

(See the 'General Principles' outlined in Section B of the Policy section, above, all of which will apply to how the Trust manages its financial data)

1. Managing financial data of *members* – bank account details etc.
2. Managing financial data of *employees* – details of income, tax, pensions etc.
3. Managing financial data of our *suppliers* – especially the security of that data.

Employees and Volunteers:

The Trust will keep under review:

1. The data held about employees – *this will comprise records relating to the appointment process; salary; terms and conditions of employment; pension arrangements; job reviews; disciplinary issues etc.*

2. *How* the data is used.
3. *Why* the Trust needs to *continue holding this data.*
4. *Where* this data is kept so that it is *confidential, secure* and *only available to those who need to have access to it.*

The Trust will set up:

1. A *log of data* that is held.
2. A system of *informing employees and volunteers of what data is held on them*.

Data Storage:

1. Data will be stored in as *few places as necessary,* with *duplicate data sets* reduced to the bare minimum to guard against loss by fire or other accidental cause.
2. Where data is stored on *paper* it will be in *secure locked storage in the* Main Office where unauthorised persons cannot access it. This applies to both original documents and print-outs from computers and will include data from the WEX and Phoenix groups and the Conservation Team.
3. Print-outs will *never be left where unauthorised persons might find them*, for example, in a printer or photo-copier.
4. Data print-outs will be *shredded and disposed of* when no longer required.
5. Electronic data will be protected by *strong passwords* which will be *changed regularly* and never given out to employees or volunteers who do not need to know them.
6. Employees or volunteers will ensure that *the screens of their computers are cleared* if they have been working on personnel or financial data and are then planning to be away from their computers, even for short period of time.
7. Any data stored on *CDs, DVDs* or *external hard drives* will be kept *securely locked away*.

8. Data will only be stored on *designated drives and servers* and if a *'cloud' storage* method is used, this will be of an approved type.
9. Data will be *backed-up* on a regular basis.
10. Data will never be saved onto *personal lap-tops or other mobile devices* such as tablets or smart phones.
11. All computers containing data will be protected by approved *security software* and a robust *firewall.*
12. Personal data on members, or financial data, *will never be sent by e-mail except under exceptional circumstances* as this form of communication is often insecure.
13. The practice of having *publicly-viewable sign-up sheets for holidays*, which ask for members contact details, will be replaced by a *system of booking slips* to be completed and posted into a secure box.
14. Related to this, *group e-mails* sent out to members (for example, participants in trips or other activities) will be done using *'blind copy' (Bcc) methods*.
15. The Trust will use the *Mailchimp bulk mailing service* to send out electronic versions of members' newsletters and other documents. Mailchimp's privacy policy is available at www.mailchimp.com/legal/privacy/

~~~~~

Original document was drawn up by Ken Chapman, Chair of Trustees, March 25th 2018 and approved by the Observatory Council on April 16th 2018. Reviewed by Council September 2019. Added to Handbook June 2022.
~~~~~