BSBI Data Handling Policy

Prepared by and date:	Julia Hanmer, June 2021
Reviewed by and date:	Trustees approved at the 22 June 2021 Board meeting
Next Review Date:	Spring 2022 (Annual review cycle)

This policy sets out the internal data handling policy for the BSBI in relation to personal data collected and processed by the organisation.

Policy

1. Context and Risk Management

i. BSBI is a charity made up of members, volunteers, trustees and staff and, as such, must collate and handle personal data in order to deliver its charitable objectives

ii. BSBI has a duty to ensure that data is only collated and stored when it is necessary to do so, with the understanding of the individuals to whom data relates, and to ensure that the data is handled securely and disposed of when no longer required.

iii. The public is increasingly subjected to stories related to breaches of trust and legislation where personal data is concerned and its perception of a charity and its moral and ethical behaviour is critical to its reputation and ability to operate and fundraise successfully.

2. Definitions

i. Personal Data - defined as data which allows an individual to be identified, including: name,membership number, postal address, email address and phone number, age or bank details.

ii. Sensitive Personal Data - defined as information relating to: ethnic background, political opinions, religious beliefs, health, sex life or criminal records.

iii. Data Notice - defined as a short, clear statement informing people why personal data isbeing collected and how it will be treated.

iv. Serious Data Breach - defined as a breach of security, either accidentally or deliberately,that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. Application and Exclusions

i. This policy applies to all BSBI members, volunteers, trustees and staff who provide, request, hold or use personal membership data on behalf of BSBI.

4. Legal framework

The BSBI Privacy Policy has been drawn up having regard to:

i. Data Protection Act 1998

ii. Freedom of Information Act 2000

iii. UK General Data Protection Regulation (UK GDPR)

iv. Privacy and Electronic Communications Regulations (PECR)

v. The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

Our data handling must respect the requirements of each of these pieces of legislation.

Following the exit of the UK from the EU, our activities in the Republic of Ireland are governed by a separate EU GDPR. The BSBI is responsible for data that is being collected and processed in both the UK and the EU. At present, the UK GDPR and EU GDPR are almost synonymous, but this may change in future. Data is able to be transferred between the UK and EEA without additional processes or permissions.

The EU is in the process of considering whether the UK can be covered by longer standing adequacy regulations, which would safeguard the simple transfer of data between the EU and UK.

5. We recognise that:

i. It is necessary for BSBI to hold personal data in order to function as an active membership society, deliver its charitable objectives and employ the staff that support this.

ii. It is necessary for BSBI to hold limited amounts of sensitive personal data on staff and volunteers in order to follow best practise in regards safeguarding, as set out in our Safeguarding Policy, to manage staff and volunteers, and to deliver on strategic goals. We describe how we handle sensitive personal data in Procedures 1.iv below and the Personal Data Processing Log (Appendix 2).

iii. BSBI must be clear in telling people why we are collecting and processing personal data and how it will be treated, as part of a Privacy Policy, which is published on our website.

iv. Where BSBI holds data on an individual, it will be deleted when it is no longer required for the purpose it was collected for (as covered by the Privacy Policy) or sooner if requested by the individual the data relates to.

v. We have a duty to abide by standard data protection principles, as defined by the Data Protection Act 1998 and following legislation, and ensure that information is:

1. Used fairly and lawfully
2. Used for limited, specifically stated purposes
3. Used in a way that is adequate, relevant and not excessive
4. Accurate
5. Kept for no longer than is absolutely necessary
6. Handled according to people's data protection rights
7. Kept safe and secure
8. Not transferred outside the European Economic Area without adequate protection

vi. It is in the best interests of individuals, the BSBI and all handling data that data be stored securely, not be duplicated, not be used in ways that it was not intended for, not stored for longer than necessary, not downloaded or stored unnecessarily, not transferred unnecessarily or shared with parties who have no legitimate need to access it.

6. We will seek to keep personal data safe by:

i. Adopting the standard data protection principles as set out in Section 5.

ii. Adopting a series of related procedures as set out below.

iii. Where necessary to pass data to third party data processors, ensuring there are adequate checks, contracts and safeguards in place to ensure they follow data protection and GDPR legislation and best practice.

iv. Communicating regularly with those who hold and process personal data on behalf of BSBI and advising them of our policy and procedures.

v. Keeping these policy and procedures under review.

7. Related Documents

i. BSBI's Privacy Policy
ii. BSBI's Staff Handbook
iii. BSBI's Safeguarding Policy
iv. BSBI's Governance Handbook (in preparation, 2021)

8. Enforcement

i. Any breaches of this Policy must be reported to either BSBI's Data Protection Officer (Chief Executive) or Chair of the Board (see www.bsbi.org/whos-who for details) as soon as recognised.

ii. If a breach is deemed significant it will be reported to the Information Commissioners Office.

iii. A breach of this Policy by staff may be regarded as a disciplinary offence under BSBI's Staff Disciplinary Procedures.

Procedures

How data must be handled, transferred, stored and deleted

1. How BSBI processes personal data

i. BSBI only holds and processes personal data for the reasons outlined in the Privacy Policy. These are:

- where clear consent has been given for us to do so.
- where we have a contractual obligation to fulfil.
- where we have a legitimate interest to fulfil our charitable aims.

Where we process personal data on the basis of our legitimate interests, we do so for the following purposes:

- to manage member, volunteer, donor, staff and external relationships.
- to tailor our communications to work we believe the individual may find interesting or may wish to support, respecting their contact preferences.

ii. BSBI keeps a Personal Data Processing Log (see below) to track all sources of data it processes; documenting what data it holds, where, how and why, including the lawful basis for doing so. In doing this, BSBI is confident that it is compliant with legislation

relating to personal data as directed by the UK GDPR.

iii. The Data Protection Officer is responsible for maintaining the Personal Data Processing Log in line with organisational developments and the annual review of the Privacy Policy.

iv. The majority of data that BSBI processes may be personal but not sensitive, the exception being Disclosure and Barring Service (DBS) information returned in relation to the two Safeguarding Leads and limited personal information relating to the health of staff.

v. Third party data processors must be thoroughly vetted before they are used to ensure they adhere to Data Protection and GDPR regulations, and their use signed off by the Data Protection Officer. Examples of existing third party data processors include:

- The membership database, currently Subscriber
- Our automated email platform, currently MailChimp
- Our payment software for memberships, publications and events, including Paypal
- Google Analytics to monitor our website statistics

vi. BSBI will maintain a log of any data breaches that occur and will report any serious data breaches (as defined above) to the appropriate authority.

2. All those that have agreed access to data must:

i. Observe this Policy and related procedures and keep themselves informed of any updates to it.

ii. Only process personal data where appropriate and necessary for their role and duties, and as described in the Personal Data Processing Log.

iii. Speak with the Data Protection Officer should they wish to process any personal data not described in the Personal Data Processing Log and ensure that appropriate permissions are obtained before any new data processing is established, whether electronic or hardcopy, and whether permanent or temporary.

iv. Produce Data Notices (see template below) on all forms of communication requesting and using data to make clear why and how the data will be treated.

v. Not hold personal data outside of an appropriate storage form (i.e. in a database or data processing system), unless its holding is required for any ongoing analysis or communications for which appropriate permission has been obtained. If using data for any purpose outside of its standard storage (i.e. downloading data from the database in order to analyse it), only hold it for as short a time as necessary and delete afterwards, ensuring any copies or circulated versions are treated the same.

vi. Conduct thorough research into any third party before it is used to process personal

data.

vii. Blind copy (Bcc) recipients when electronic communications are sent out to mailing lists. A minor exception is when putting individuals in touch with each other to arrange shared transport.

viii. Only process and record such personal data as required for the task at hand (e.g. not add personal address data to a botanical record, where only a name is required)

ix. Only transfer personal data where absolutely necessary for the fulfilment of roles, and when doing so ensure it is protected where possible (e.g. through password protection of a spreadsheet)

x. Provide, within 30 days, information on the personal data held on an individual, should they request it.

xi. Provide clear instructions on all communications to allow recipients to 'opt out' of future mailings, and ensure any changes to consent are accurately updated on the Membership Database (through the Membership Secretary) and on Mailchimp (through the Communications Manager).

xii. Thoroughly and permanently delete any personal data held on an individual, should they request it or when no longer required. This includes from databases, address books and electronic caches and in hard copy format. Care should also be taken when disposing of computer hardware previously used to process personal data.

xiii. Report all data breaches or any other data related concerns to BSBI's Data Protection Officer, Julia Hanmer.

3. All those that have agreed access to data must not:

i. Keep personal data if not necessary for the functioning of their role with BSBI.

ii. Keep personal data if not fully described on the Personal Data Processing Log.

iii. Share any personal data they hold with any other individual or organisation, whether internal or external to BSBI, unless described on the Personal Data Processing Log.

iv. Ask for, access or hold any sensitive personal data, except where required by their role.

v. Withhold information on the personal data they hold if queried by the person the data relates to or by any regulatory body.

C. Training

As and when deemed necessary, the Data Protection Officer may ask staff and volunteers who handle personal data to complete mandatory training on data security.

Appendix 1

Template Data Notice to be used on any communication, form or place where requesting data.
Text in the square brackets should be deleted or amended as appropriate.

This information is being requested [to manage your subscription/send you the publication/send you the information described/to administer the event advertised]. BSBI will only hold the information to fulfil this purpose. Please see our Privacy Policy for further details of how your data will be handled and stored. You can request to see the data we hold, request its removal or update your contact preferences at any time by contacting us. To do so, email enquiries@bsbi.org.

Appendix 2

Personal Data Processing Log

Data	Type of Data	How used	Where held	Who has access	When deleted	Lawful Basis for processing
Membership data: name, address, email, phone and payment information (directdebit, bank details etc.)	Personal data	To administer BSBI's membership and develop and distribute membership publications, benefits and updates.	Our membership database (Subscriber) and financial and accounting systems (BSBI Charity Bank Account, SAGE accounting software package, Smartdebit Direct Debit system). Where forms are submitted in hard copy (currently still an option through the website), they are held at the home of the Membership Secretary.	Membership Secretary and Fundraising Manager have individual password access. Monthly summary sent securely to Finance Manager, Communications Manager and CEO. Specified individuals (staff or members in an official voluntary role) have limited access to members' details upon approval by the CEO.	From Subscriber: Two years after membership has lapsed. From third party data processors and hard copy forms: Bank account and other personal details held electronically for members paying by DD are held only for six months and then deleted. Other financial information is deleted six years after membership has lapsed or employment ceased,as per standard accounting practice and regulations relating to Gift Aid, etc.	Contractual
Additional membership data: Date of birth, reason for joining, level of	Personal data	To fulfil our strategic goal of diversifying our membership, and to better understand the	Our membership database (Subscriber).	As above.	As above.	Legitimate interest

botanical skill		wants and requirements of the cohort in order to deliver an effective service.				
Staff data: name, address, email, contractual information and payment information (directdebit, bank details etc.)	Personal data	To fulfil HR and Safeguarding requirements.	On CEO and Line Manager laptops (on cloud storage servers) as employment contracts (digital) and in financial and accounting systems.	CEO and Finance Manager.	When individual concerned no longer holds the staff role.	Contractual
Financial information: name,address and bank account details (account number and sort code) of organisations and people paid.	Personal data	To make payments fromBSBI. This includes to staff, volunteers, sole traders, companies etc.	BSBI Charity Bank Account, SAGE accounting software package, Excel, word or PDFs, all securely stored on the Finance Officer's laptop.	Finance Manager.	Six years after used, as per standard accounting practice.	Contractual
Recruitment data: name, email, address, application information	Personal data	To facilitate the recruitment of staff and volunteer roles, including the adherence to recruitment law.	On recruiting team's laptops (on cloud storage servers).	CEO and recruiting team.	Six months to a year after application.	Contractual

Newsletter Mailing List: name, email.	Personal data	To send out monthly e-newsletter	MailChimp	Single password access, shared by Communications Manager, Scotland Officer and Database Officer.	Unsubscribe option included in every email.	Consent
Trustees / Committee Members / VCRs / Referees: Name, email, address (occasionally).	Personal data	To fulfil volunteer role.	With express permission and consent on taking up role, contact information is shared with membership, in publications and on website, and is supplied to external agencies as required (e.g. to Charity Commission).	Publicly available.	When deletion is requested by an individual or when they no longer hold a voluntary position.	Consent
Events: Name, email, address (occasionally). Payment details are processed by third party where a fee is charged.	Personal data	By event organisers in order to administer the event	On event management software (e.g. TicketTailor)	Event organiser and other internal staff members for administration. Event management software is password protected.	2 years after the event has taken place.	Contractual

Publications: Name, address. Payment details are processed by third party where a fee is charged.	Personal data	To process and fulfil order.	In Membership Database and through payment processing software. Address details may be shared securely with publishing house to fulfil orders, with no further right to use.	Database access as above. Order fulfilment details shared through Finance Manager.	When membership record is deleted and financial information removed (see above).	Contractual
Local Groups: name, email, address (occasionally).	Personal data	By nominated group leaders to administrate a local group (e.g. a County Recording Group)	On group leader's own system. The leaders are subject to the rules and provisions of this policy when holding this data and must comply with all requests for addition, deletion and amendment from BSBI and members.	Nominated group leaders who have been advised of their data protection requirements.	When deletion is requested by an individual or an updated list is provided by BSBI.	Consent
Fundraising: name, email, address. Payment details are processed by third party where a digital payment is made.	Personal data	For fulfilment of charitable aims and under provision of legitimate interest, BSBI may advertise appeals to members and contacts, respecting contact preferences.	In Membership Database and through payment processing software. Details of donors may be shared with other internal staff to facilitate the appropriate thanking and acknowledgement of gifts.	Database access as above. Donation details shared through Finance Manager.	When membership record is deleted and financial information removed (see above).	Legitimate interest

DBS checks (and the equivalent in other jurisdictions): name, address information, ID, DOB. Potential for sensitive information to be returned from DBS.	Sensitive personal data	To carry out checks in order to comply with safeguarding policy.	Password protected by CEO.	Request submitted by Chair of Board and returns passed to CEO for holding on file.	When the individual concerned no longer holds theSafeguarding Lead role.	Consent
App derived occurrence data: name, time-sensitive location.	Personal data	Input from users through recording software. See Privacy Policy for further details of processing of botanical records.	Processed through app and added to DDb (see following entry).	User has access at point of entry. Database Officer and Head of Science have overall access control.	Personal details deleted on request as per following entry.	Consent
DDb occurrence data: name, time-sensitive location.	Personal data	As part of input and verification process for botanical records uploaded to the DDb. Only the minimum amount of data required should be entered.	Within record data on password protected DDb. This data may be accessed, analysed and shared with other third party data agencies where sharing agreements have been made, as per the BSBI Data Access Policy.	Database Officer and Head of Science have overall access control. Can be downloaded as part of data sets.	Personal details deleted on request.	Legitimate interest

DDb access data: name, organisation, email.	Personal data	To grant access to the Distribution Database. Reviewed by staff to ensure suitability of access to DDb data, and used to create editable user profile.	On password protected DDb backend.	Database Officer and Head of Science. User list available to staff.	When individual requests account deletion or permission is denied.	Contractual
Website logs	Personal data (IP address)	Monitoring of website usage.	Web server (plain text log files).	Database Officer	After 60 days.	Legitimate interest
Wordpress website registrations	Personal data (name, email address)	To administer access to privileged parts of wordpress websites (bsbi.org and also conference microsites)	Web server (mysql database)	All staff	On request.	Consent

Herbarium@home registrations	Personal data (name, email address)	To administer operation of web-based project.	Web server (mysql database)	Database Officer	On request.	Consent