

Botanical Society of Britain and Ireland Data Handling Policy

Prepared by and date:	Julia Hanmer, June 2023
Reviewed by and date:	Approved by the Trustees at the 20 June 2023 Board meeting
Next Review Date:	June 2024 (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.

Contents

Policy	P1	
Procedures	P4	
Appendix 1	Template Data Notice	P6
Appendix 2	Volunteer Confidentiality and Data Protection Agreement	P7
Appendix 3	Personal Data Processing Log	P9
Appendix 4	Job Application Privacy Notice	P18

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. Personal data protection and security are an important part of our culture at BSBI. We need to ensure that our members, supporters and the community of botanists can trust us to use their data fairly and responsibly. BSBI has a duty to ensure that data are 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 are 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 are 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, trade union membership, genetic data, biometric data, health, sexual orientation, sex life or criminal records.
- iii. Data Notice - defined as a short, clear privacy statement informing people why personal data are being 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 Data Handling and Privacy Policies have been drawn up having regard to the following legal frameworks:

- a) The UK:
 - i. Data Protection Act 2018
 - ii. Freedom of Information Act 2000
 - iii. UK General Data Protection Regulation (UK GDPR) the retained EU law version of the GDPR
 - iv. Privacy and Electronic Communications Regulations (PECR)
 - v. The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
- b) The Republic of Ireland:
 - i. General Data Protection Regulation (GDPR)
 - ii. The Data Protection Act 2018
 - iii. The Data Protection Acts 1988 and 2003
 - iv. 2011 ePrivacy regulations

Our data handling must respect the requirements of each of these pieces of legislation and guidance produced by the [Information Commissioners Office](#) (UK) or [the Data Protection Commission](#) (Ireland).

The BSBI, by virtue of its jurisdiction, operates in the UK and the Republic of Ireland. Following the exit of the UK from the European Union, transfers of personal data remain unrestricted within the EEA under 'adequacy regulations' as long as processing continues to meet the requirements of the GDPR. At present, the UK GDPR and EU GDPR are almost synonymous, but this may change in future, in which case this policy will be updated.

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 3).
- 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 and Personal Data

Processing Log) 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 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 UK or 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 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 Policies (for Children and Young People and Adults)
- iv. BSBI's Governance Handbook (in preparation)

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](#) (UK) or [the Data Protection Commission](#) (Ireland).
- 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 Appendix 3) 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 legislation outlined in section 4 above.
- 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 to the Designated Safeguarding Lead to comply with safeguarding policy and limited personal information relating to the health of event participants to ensure their safe participation or the health of staff to ensure safe working practices.
- v. Third party data processors must be thoroughly vetted before they are used to ensure they adhere to Data Protection regulations, and their use signed off by the Data Protection Officer. Examples of existing third party data processors include:
 - The membership database, currently Beacon
 - Our automated email platform, currently MailChimp
 - Our various payment software/portals for memberships, publications and events (see Personal data processing log for more details)
 - Google Analytics to monitor our website statistics
 - Accounting software, currently Sage
 - Banking portals, currently CAF Bank and HSBC
- 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 (Appendix 3).
- 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, data processing or accounting 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 Officer).
- xii. Thoroughly and permanently delete any personal data held on an individual, should they request it or when no longer needed or required to be held (e.g. as part of accounting records). 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. Hold personal data within accounting records (e.g. bank account details) for no longer than the 6 years legally required <https://www.gov.uk/running-a-limited-company/company-and-accounting-records>.
- xiv. 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.

4. 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

BSBI Volunteer Confidentiality and Data Protection Agreement

Working with data

Personal data protection and security is an important part of our culture at BSBI. We need to ensure that our members, supporters and the community of botanists can trust us to use their data fairly and responsibly. As a Data Controller, BSBI has a responsibility to work appropriately and correctly with data of all kinds. Through undertaking one of the volunteer roles that enable BSBI to fulfil its charitable purpose, you may come into contact with personal information that has been entrusted to BSBI by other individuals.

The BSBI operates in the UK and the Republic of Ireland, so how we collect, manage and work with people's information is covered by the General Data Protection Regulation (GDPR and UK GDPR) and the Data Protection Acts of both the UK and the Republic of Ireland. The charity, staff and volunteers all have a role to play to ensure we maintain the highest standards regarding Data Protection.

You have been identified as taking on a role that will have a degree of contact with personal data and therefore we ask you to complete this form acknowledging you understand your responsibilities towards safe data management and confidentiality. You should ensure you read and understand our **Privacy Policy** as well as our **Data Handling Policy**, including any subsequent updates that may be circulated. If you have any questions or would like support in understanding the function of data protection within your role, BSBI staff will be able to help you. Periodically it may be necessary for you to undergo further training to ensure we maintain the highest principles in data management.

The types of data you could come into contact within your BSBI volunteer role are categorised as follows:

- Name
- Contact details (e.g. Address, Email address)
- Age
- Health information (sensitive personal data - see below)
- Photographs
- Level of botanical skill (self-assessed)
- Reason for joining an activity
- Grant application details
- For committee recruitment: Volunteer role applications and self-assessment against competency frameworks and diversity surveys.
- For Field Identification Skills Certificates (FISCS), botanical assessment scores

It is not expected that you should handle any data classified as 'special category' or 'sensitive personal data', aside from where an individual may disclose health information to you for the purposes of attending an event safely (e.g. accessibility or dietary requirements).

Information should only be gathered from individuals with their consent and that which is specifically needed for a given purpose, and those who collect the data need to ensure they only use it for BSBI purposes (use for any other purpose would be information theft under the data protection legislation), have robust procedures in place to ensure it is held in a safe and secure format (for example password protected). Information must be deleted upon request or vacation of role, and no backup copies restored to foreground.

If you ever become aware of a data breach, or if there is a risk of a breach, please notify the Data Protection Officer, Julia Hanmer immediately by emailing julia.hanmer@bsbi.org or calling 07757 244651. This is important so we can continually review and improve the way we work. Please note that BSBI is under a legal obligation to share evidence of misuse of personal data with the [Information Commissioners Office](#) (UK) or [the Data Protection Commission](#) (Ireland).

Confidentiality

The charity owes a duty of confidentiality to the people we hold information about and is an essential principle of the services we provide to ensure that the people and organisations we work with trust us. Confidentiality is important even if a situation might seem informal, for example correspondence through emails, committee papers and minutes, the organisation of an event, training course or assessment, or information relating to ongoing research projects. If you have more than one volunteer role within BSBI, information in these categories should be kept confidential within an individual role.

Organisation policies on safeguarding and health and safety may also determine when confidential information may need to be shared. Julia Hanmer, Data Protection Officer for BSBI, can help with anything that you're unsure about around these issues and training is available.

Statement

As a volunteer with the Botanical Society of Britain and Ireland I have read and agree to follow the BSBI's Privacy and Data Handling Policies. I will not discuss confidential information which I gain access to through delivering my role, send it by any means to any third party unless I am explicitly authorised to do so, or share it in general conversation or use it for my own purposes whilst in my role or once my role has ended. I will delete data upon request. On ending my role at BSBI I will either pass data back to BSBI staff or delete it and I will ensure that no backup copies restored to foreground.

I have read and I agree to comply with the above agreement and its associated policies:

Volunteer Name:		Volunteer Role: (formal role or active member)	
Type of data requested: (Eg. Member contact emails for x area)		Reason for data request:	
Signature:		Date:	

About BSBI: The Botanical Society of Britain and Ireland (BSBI) is a company limited by guarantee registered in England and Wales (8553976) and a charity registered in England and Wales (1152954) and in Scotland (SC038675). Registered office: 28 Chipchase Grove, Durham DH1 3FA.

Privacy statement

We'll only use the information you've given us to implement our data protection procedures. It will be treated as confidential and stored in line with data protection legislation. Please see our [Privacy Policy](#) for more information about how we look after your data.

Appendix 3

Personal Data Processing Log

Data	Type of Data	How used	Where held	Who has access	When deleted	Lawful Basis for processing
<p>Membership data: name, address, email, phone, payment information (Direct Debit, bank details etc.), language preferences</p>	Personal data	To administer BSBI's membership and develop and distribute membership publications, benefits and updates.	Our membership database (Beacon) and financial and accounting systems (BSBI's CAF Bank Portal, SAGE accounting software package, Go Cardless & Stripe).. Where forms are submitted in hard copy (currently still an option through the website), they are held at the home of the Membership Secretary.	The Membership Secretary, Finance Manager and Fundraising Manager operate Administrator rights to the database. Other staff, where required by their role, are provided with regular access rights. Specified individuals (staff or members in an official voluntary role) may be given limited access to specific members' contact details upon approval by the CEO (on signing the agreement in Appendix 2)	<p><u>From Beacon:</u> Two years after membership has lapsed.</p> <p><u>From third party data processors and hard copy forms:</u> 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.</p> <p>https://www.gov.uk/running-a-limited-company/company-and-accounting-records</p>	Contractual

Additional membership data: Date of birth, reason for joining, level of botanical skill	Personal data	To fulfil our strategic goal of diversifying our membership, and to better understand the wants and requirements of the cohort in order to deliver an effective service.	Our membership database (Beacon).	As above.	As above.	Legitimate interest
Newsletter Mailing List: name, email, botanical skill level.	Personal data	To send out monthly e-newsletter	Membership Database.	As above under Membership data.	Unsubscribe option included in every email.	Consent
Staff data: name, address, email, emergency contact, contractual information and payment information (directdebit, bank details etc.) Health information (occasionally)	Personal data Health information is sensitive personal data	To fulfil HR and Safeguarding requirements.	On CEO, Finance Manager and Line Manager laptops (and on cloud storage servers) as employment contracts (digital) and in financial and accounting systems.	CEO, Finance Manager, Line manager.	When individual concerned no longer holds the staff role at BSBI – within a year of their leaving date.	Contractual

Financial information: name, address and bank account details (account number and sort code) of organisations and people paid.	Personal data	To make payments. This includes to staff, volunteers, sole traders, companies etc.	BSBI's Banks (CAF Bank and HSBC), SAGE accounting software package, Excel, Word or PDFs, all securely stored on the Finance Manager's laptop.	Finance Manager.	Six years after used, as per standard accounting practice. https://www.gov.uk/running-a-limited-company/company-and-accounting-records	Contractual
Recruitment data (staff roles): name, email, address, phone, qualifications, skills, experience, employment history and information about disability, right to work in the UK/Ireland and criminal convictions	Personal data and Sensitive personal data	To facilitate the recruitment of staff roles, including the adherence to recruitment law, equality law, safeguarding policy. On advertising staff roles the "BSBI Job Application Privacy Notice" (see Appendix 4) is shared along with the recruitment pack	On recruiting team's laptops (on cloud storage servers). Applications are anonymised and sensitive personal data is removed for the selection stage.	CEO and recruiting team. Sensitive personal data will only be shared on a need to know basis	For those not recruited: Six months to a year after application. For those recruited: until they leave the role.	Contractual

Recruitment data (volunteer roles): name, phone, application information	Personal data	To facilitate the recruitment of volunteer roles, including the adherence to recruitment law	On recruiting team's laptops (on cloud storage servers)	CEO and recruiting team	For those recruited: until they leave their voluntary role at BSBI For those not recruited: Within 1 year of application	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 other committee members, the BSBI membership, users of BSBI recording apps, 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
Trustees / Committee Members Name, email, self-assessment against a committee competency and diversity framework or survey.	Personal data	To fulfil our strategic goals of strong governance and diversifying our membership, plus to better understand the support and development needs of our volunteers	Password protected document	CEO, Committee Chair, Committee Secretary	On request Self-assessments deleted once analysed into summary level information for committees, with no personal data included.	Consent

<p>Events: Name, email, address (occasionally). Payment details are processed by third party where a fee is charged.</p>	<p>Personal data</p>	<p>By event organisers in order to administer the event</p>	<p>On event management software (e.g. TicketTailor) and Membership Database (Beacon).</p>	<p>Event organiser and other internal staff members for administration. Password protected event management software; password protected document where details are passed to Event organiser.</p>	<p>2 years after the event has taken place.</p>	<p>Contractual</p>
<p>BSBI Event participant or Local Group members: name, email, address (occasionally), health information (occasionally).</p>	<p>Personal data Health information is sensitive personal data</p>	<p>By nominated BSBI event or local group leaders to administrate a local group (e.g. a County Recording Group) or event (e.g. a local field trip)</p>	<p>On Group/Event 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.</p>	<p>Nominated Group/Event leaders who have been advised of their data protection requirements.</p>	<p>When deletion is requested by an individual or an updated list is provided by BSBI.</p>	<p>Consent</p>
<p>Publications: Name, address. Payment details are processed by third party where a fee is charged.</p>	<p>Personal data</p>	<p>To process and fulfil order.</p>	<p>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.</p>	<p>Database access as above. Order fulfilment details shared through Finance Manager.</p>	<p>When membership record is deleted and financial information removed (see above).</p>	<p>Contractual</p>

<p>Fundraising: name, email, address. Payment details are processed by third party where a digital payment is made.</p>	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
<p>DBS checks (and the equivalent in other jurisdictions): name, address information, ID, DOB. Potential for sensitive information to be returned from DBS.</p>	Sensitive personal data	To carry out checks and risk assessments in order to comply with safeguarding policy.	Stored offline and password protected by CEO (Designated Safeguarding Lead)	Request submitted by Board Safeguarding lead or CEO (Designated Safeguarding Lead) and returns passed to CEO for risk assessment and holding on file.	When the individual concerned no longer holds the Safeguarding Lead role. Prior data will be passed to the new Designated Safeguarding Lead.	Consent
<p>App derived personal data: Name, email address, home-town or country</p>	Personal data	Input from users through recording software account details page. Used to suggest recorder names to other app users.	Processed through the app and added to BSBI's Distribution database (DDb)	Users of BSBI's recording software	Personal details on request	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 (Distribution Database) 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 microsities)	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
FISC (Field Identification Skills Certificate) Name, email, assessment scores and overall FISC level.	Personal data (name, email address, FISC scores and level.	To administer, coordinate and quality control FISC assessments of botanical field skills.	Protected shared drive, Membership Database (Beacon), password protected documents (where being communicated to Joint Data Controllers)	Skills and Training FISC sub group; CEO and staff involved in FISC coordination; FISC local Providers (Joint Data Controllers)	On request	Contractual

Identiplant training course Name, email, postcode, location (county)	Personal data (name, email address) and course evaluation details	To administer, coordinate and quality control the Identiplant training course.	Protected shared drive and Membership Database (Beacon)	Skills and Training Identiplant sub group, CEO and staff involved in Identiplant coordination and Identiplant Tutors	On request	Contractual
Grants Name, email and grant application details	Personal data (name, contact and grant application details, payment details)	To administer BSBI's Grants for Training, Plant Study, Science and Research)	Password protected spreadsheets	Committee subgroups for grant decision making; Communications Officer, Finance Manager and relevant staff for administration, payment and reporting	On request	Consent

Appendix 4

BSBI Job Application Privacy Notice

Data Controller: Botanical Society of Britain and Ireland (BSBI), 28 Chipchase Grove, Durham DH1 3FA.

As part of any recruitment process, BSBI collects and processes personal data relating to job applicants. BSBI is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does BSBI collect?

BSBI collects a range of information about you. This includes:

- Your name, address and contact details (including email address and telephone number)
- Details of your qualifications, skills, experience and employment history
- Information about your current level of remuneration
- Whether or not you have a disability for which BSBI needs to make reasonable adjustments during the recruitment process
- Information about your entitlement to work in the UK
- Information about criminal convictions and offences

BSBI may collect this information in a variety of ways. For example, data might be contained in application forms, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment.

BSBI may also collect personal data about you from third parties, such as references supplied by current or former employers and information from criminal records checks.

BSBI will seek information from third parties only after the interview stage and after permission has been sought from you. Data will be stored in a range of different places, including your application record, in HR line management systems and on other IT systems (including email).

Why does BSBI process personal data?

BSBI needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data in order to enter into a contract with you. In some cases, BSBI needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

BSBI has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows BSBI to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. BSBI may also need to process data from job applicants to respond to and defend legal claims.

BSBI may also collect information about whether or not applicants are disabled in order to make reasonable adjustments for candidates who have a disability. BSBI processes such information to carry out its obligations and exercise specific rights in relation to employment.

For some roles, BSBI is obliged to seek information about criminal convictions and offences. Where BSBI seeks this information as a vital interest, it does so because it is necessary for it to carry out its

obligations and exercise specific rights in relation to employment and the protection of the public, children and young people and vulnerable adults.

BSBI will not use data that will identify you for any purpose other than the recruitment process for which you have applied. If you are successful your application will be transferred into a personnel file.

Who has access to data?

Your information may be shared internally for the recruitment process. This includes members of the BSBI staff team and interviewers involved in the recruitment process, if access to the data is necessary for the performance of their roles. Where the post is funded by an external partner, or involves partnership working, a representative from the funder or partnership may be involved in the recruitment process. In such cases, your information will also be shared with them.

BSBI will not share your data with any other third parties, unless your application for employment is successful and it makes you an offer of employment. BSBI will then share your data with current and former employers to obtain references for you, and, if appropriate to the role, the Disclosure and Barring Service to obtain necessary criminal records checks. BSBI will not transfer your data outside the European Economic Area.

How does BSBI protect data?

BSBI takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties. Information will be stored securely in electronic files.

How long does BSBI keep data?

If your application for employment is unsuccessful, BSBI will hold your data on file for 6 months after the end of the relevant recruitment process. At the end of that period your data will be deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The period for which your data will be held after you leave BSBI is set out in [BSBI's Data Handling Policy](#).

Your rights

As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request
- Require BSBI to change incorrect or incomplete data
- Require BSBI to delete or stop processing your data, for example where the data is no longer necessary for purposes of processing
- Object to the processing of your data where BSBI is relying on its legitimate interests as the legal ground for processing

If you would like to exercise any of these rights, please contact Julia Hanmer, Chief Executive, Julia.Hanmer@bsbi.org

If you believe that BSBI has not complied with your data protection rights, you can complain to the Information Commissioner (UK) or The Data Protection Commission (Ireland)

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to BSBI during the recruitment process. However, if you do not provide the information, BSBI may not be able to process your application properly or at all.

Automated decision-making

Automated decision-making plays no part in BSBI's recruitment processes.

About BSBI

The Botanical Society of Britain and Ireland (BSBI) is a company limited by guarantee registered in England and Wales (8553976) and a charity registered in England and Wales (1152954) and in Scotland (SC038675). Registered office: 28 Chipchase Grove, Durham DH1 3FA.