Butterfly Conservation

Saving butterflies, moths and our environment

Branch Data Protection Guidelines

Contents:

1. Background Information

This document aims to provide information and guidance for Branches on Data Protection and should be read in conjunction with Butterfly Conservation's existing Data Protection Policy Statement, Data Protection Guidelines and Procedures for Handling Personal Information.

The Data Protection Act 1998 defines the UK law on the processing of data on identifiable living people. The Act protects people's right to privacy with respect to the processing of personal data and provides a way for individuals to control information about themselves. Electronic communications are regulated by the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

Butterfly Conservation is licensed with the Information Commissioner as a data controller. ALL personal data held by Butterfly Conservation staff, Branches and volunteers is covered by the Data Protection Act. The Act is mandatory so it is essential that we all comply with it. A breach of the regulations could result in compensation claims, prosecution, huge fines, bad publicity and damage to our reputation.

The definition of personal data is any information about a living individual from which they can be identified, eg name, address, email address etc and includes information held by paper copy, electronically or in any other recorded media.

A brief summary of the key principles required to ensure good practice are:

- Data may only be used for the specific purposes for which it was collected.
- Data should not be disclosed to other parties outside of BC without the consent of the individual.

- Individuals have a right of access to the information held about them.
- Personal information is kept for no longer than is necessary and should be kept up to date.

- Personal information should not be sent outside the European Economic Area (EEA) (unless specific procedures have been followed). If any Branch wishes to send personal data outside the EEA please contact Head Office.

- All departments or individuals holding personal information are required to have adequate security measures in place. These include technical measures such as firewalls etc, and appropriate guidance or training.

- Individuals have the right to have factually incorrect information corrected.

2. Personal data held at Head Office

The majority of data held for BCs members and contacts is stored on our membership database at Head Office. Access to this database is password protected and restricted to those who require it specifically for their job, eg the Membership and Administration teams.

Whenever we are notified of a change of contact details the database is updated, this should therefore always be considered the most accurate and up-to-date information held. We have a duty to ensure the information we store is correct and therefore it is imperative that any changes notified to the Branch are passed as quickly as possible to Head Office.

We currently hold email addresses for approximately one fifth of the membership on the database. The majority of these addresses were provided when members joined. We have not yet begun contacting members electronically and therefore it may be possible that some email addresses are no longer valid.

3. Transfer of data between Head Office and Branches

Member information is currently sent from Head Office to Branch Membership Secretaries by hard copy via the Royal Mail or electronically in an encrypted and password protected spreadsheet.

A report giving details of all new and leaving members is sent monthly from October to March and fortnightly from April to September. Information about changes of address etc and change of Branch are also given at this time. Up until now these reports have mainly been sent by post and contain members' names, addresses and telephone numbers only. Once the Branch Data Protection Guidelines have been read and agreed by Branch Committees we will be able to include members email addresses on the lists so that Branches can communicate electronically with members if they so wish.

Please advise Catherine Levett (clevett@butterfly-conservation.org) if your Branch Membership Secretary would like to receive reports electronically in the future.

A full list of members is sent to all Branch Membership Secretaries annually in April. However, we can provide Branches with member information as and when required at other times of the year on request.

Please note all member and contact personal data should be treated as confidential and only provided to other Branch Committee members on a strict need to know basis (see Section 6 for more information about access to data).

If Branches receive notification of updated contact information for a member they should forward to Catherine Levett (clevett@butterfly-conservation.org) so that the master database can be amended as soon as possible.

4. Data Protection statements and options to unsubscribe

Data protection statements are used to ensure that the member or contact has given permission to be contacted by post or email. It is best to keep the statements as generic as possible to allow a variety of communications to be sent from BC on different topics if required in the future.

Data protection statements are handled differently for post and email.

An **opt-out** is required for all **post/paper mail** and an **opt-in** is required for all **email** communications. Although this can sometimes cause confusion it is considered standard good practice.

Post or paper communications
BC's current standard data protection opt-out statement for post/paper is as follows:

> **Opt-out for mail**
> *From time to time we would like to send you information by post about our conservation, membership and fundraising activities. If you prefer not to receive information by post please tick this box [ ].*

A member will only tick the box if they **do not** wish to receive information by post.

Email communications
When gathering email addresses (eg at events or on forms) an opt-in statement for email should be included as follows:

> **Opt-in for email**
> *By providing your email address you agree to us contacting you by email. You can opt-out at any time in the future.*

A member should then only provide their email address if they are happy to receive information by email.

This generic opt-in statement enables us to send various electronic communications, including Branch newsletters*****, information about Branch events, field trips and AGMs, fundraising appeal information etc.

***Please note that if your Branch wishes to send electronic newsletters or annual reports to members instead of hard copy newsletters they must also check that individual members are happy to stop receiving paper copies by post.**

Both data protection statements should also include the following wording:

> ***Butterfly Conservation will not disclose any of your personally identifiable information, except when we have your permission.***

If you do not wish to use the standard data protection statements above please contact Sandra Muldoon at Head Office (smuldoon@butterfly-conservaton.org) to discuss alternative wording.

The overriding aim of a data protection statement is to ensure the individual's consent is **freely given and informed**, ie the individual is clear about what he/she is consenting to his/her data being stored for.

Once permission has been given you do not need to request it again in the future unless you intend to use the data for a completely different purpose. The generic data protection statements above would cover the majority of BC communications that the Branch or Head Office would wish to send.

Unsubscribing to email communications

It is very important that an opportunity to **unsubscribe** (ie stop receiving emails in the future) **is provided in every message** by adding the following standard wording in your footer or signature block:

> *If you do not wish to receive further emails in the future from Butterfly Conservation (insert your Branch name here) xxxx Branch please reply to this email with the words "unsubscribe" in the subject line.*

If you receive a request to unsubscribe from any member or contact you must ensure that their email address is removed from your mailing list. **Please note if we do not adhere to a request to stop email communication we could be in breach of the Data Protection Act and liable to heavy fines and ensuing bad publicity.**

5. Storage and security of personal data

All personal data should be treated with strict confidentiality.

Hard copies of member and contact name and address details should be filed securely in a locked cabinet or drawer where they cannot be accessed by anyone else.

It is useful to remember that even a post-it note with a members name and address on is classed as personal data and should be treated accordingly.

If the data is stored on a computer or laptop, it must have an Internet Security package installed that includes antivirus and antispyware protection and a firewall. Access to the computer or User Account should be password protected. Updates should be switched to Automatic and you should ensure the latest updates are installed.

The electronic file containing the personal data (e.g. Excel spreadsheet) should be stored in an encrypted location. You can add the file to an encrypted Zip file using free 7Zip software or WinZip. Simply password protecting an Excel or Word file is not secure but if you store the file in a password protected Zip file using 7Zip or WinZip this adds secure AES 256 bit encryption (see guidance below about choosing a secure password). Please be aware that it is the Zip file that is encrypted and not the personal data file so if you extract (unzip) the file to another location it is not encrypted – therefore always ensure you only store the personal data file in the password protected Zip file.

If the data is stored on an external hard-drive or memory stick it must also be encrypted.

If data is stored on a laptop or memory stick or external hard-drive please be aware of the additional potential risks of losing or misplacing the data and make special arrangements to minimise the risks.

Do **not** store names, postal addresses or email addresses of contacts within your email client software (e.g. Outlook) because the personal data will not be encrypted and some viruses automatically send out spam emails to everyone in your email address book.

If you require guidance on importing email addresses into your client software to enable you to undertake bulk email messages please contact the IT Team at Head Office (itdepartment@butterfly-conservation.org).

You must take precautions to ensure that any personal data stored electronically cannot be accessed by anyone else.

The above storage and security measures also apply to any backups of the data you make.

When choosing a password to secure your computer or file it is important to make sure the password is secure. There are a few simple things to bear in mind when creating a password 1. Make your password as long as possible, 2. Avoid using personal information that would be easy for others to guess such as your name or address, 3. Avoid obvious passwords that are easy to guess (qwerty, password, letmein, 12345 etc). See the following website for advice on choosing a secure password: http://www.microsoft.com/security/online-privacy/passwords-create.aspx

If you are sending a secure file to someone else do not use the same communication method to send them the password. For example if you send a passworded 7Zip file in an email, do not attach the password to the same message. The best thing to do would be telephone the recipient and verbally tell them the password. Although a separate email would do.

If you have any queries regarding security of data including instructions for using 7Zip software for encryption then please contact the IT Team at Head Office (itdepartment@butterfly-conservation.org).

6. Forwarding members personal data to other Branch Committee Members & restriction of data access

If the appropriate data protection statements have been used to collect the data, details of members and contacts held by Branch Membership Secretaries can be forwarded to another Branch Committee member when required for a specific purpose or mailing etc. However, personal data should always only be accessed if **needed** and not just for information. When forwarding data electronically you should ensure the file is encrypted in line with the security measures detailed in section 5.

Unless needed for future communications on a regular basis the data should be destroyed or deleted immediately after use (see section 8 below).

All Committee Members who are in receipt of members' personal data must have read and agreed to abide by these guidelines especially with regard to security, confidentiality and updating data.

Data may only be used to send communications on Butterfly Conservation business. **On no account can emails or letters be sent on behalf of non-BC organisations or non-associated events.**

7. Information held by Branch Recorders

Branch Recorders may also need to store personal data if provided on recording forms. The data protection statement on a recording form can be quite specific and if this is the case the contact information should **not** be passed to other Committee Members for communication about any other matter.

As it is essential for Branch Recorders to have the ability to contact the individual it is necessary to include the following statement on the recording form:

Butterfly Conservation may contact you about your records.

This makes it clear that if they send a record they may be contacted about it in the future.

8. Use and frequency of sending emails

Members and contacts must opt-in (see section 4 above) to receive electronic communications and must be given the opportunity to unsubscribe from receiving emails in **every** message sent.

The "bcc" facility (blind copy) should be used when sending emails to more than one member or contact. This ensures that recipients cannot see other email addresses and thus enables you to protect the addressees' privacy and comply with the requirements of the Data Protection Act. Address the message to yourself and then include the addresses of the other recipients in the "bcc" line.

The Branch must ensure that the number of emails sent to members is **strictly controlled** so that ideally no individual receives more than one message per month from a Branch. As more and more people begin communicating electronically this will become increasingly important to minimise the risk of people unsubscribing in the future. This will be easier to control if the number of Branch Committee members holding email addresses is restricted and one person is made aware when and what communications are being sent.

Some members belong to more than one Branch and therefore could receive multiple email communications. Over the coming months as more Branches begin communicating electronically with members we will keep the frequency of communications under review and monitor any complaints received from members. Please inform Sandra Muldoon (smuldoon@butterfly-conservation.org) at Head Office if you receive a complaint or query about any BC communications or our Data Protection Policy.

Emails should be kept short and to the point whenever possible. You should ensure the subject header is clear and if feasible includes "Butterfly Conservation" in the title. This will hopefully help increase the "opening rate" of your message and make sure it is seen by the maximum number of recipients.

Avoid using any language or terms in the email that may be misconstrued as Spam to minimise the chances of your emails being blocked by anti-spam services.

9. Data destruction policy

Personal data must not be held for longer than necessary. Old or out of date information should be destroyed as soon as updated details have been received.

Paper copies of information including member lists and any correspondence containing personal data should be shredded or securely disposed of.

When deleting electronic information from your computer please check it has also been removed from the Recycle Bin too. Please note that even when you delete a file from the Recycle Bin it hasn't actually been deleted from the computer's hard-drive and can be retrieved using UNDELETE software tools. Therefore before giving away or selling your computer, laptop, hard-disk or external hard-drive to anybody you should use a software tool to ensure all data has been securely erased.

Quick summary

Please be assured that these data protection guidelines are not intended to make communications more difficult but are in place to ensure we comply with legal requirements. They help safeguard those of us who deal with personal data and provide a way for individuals to control information held about them.

Main points to consider:

1. Data should only be used for the purpose it has been collected for.
2. Data should not be passed to any third party outside of BC.
3. Data should be held in a secure and confidential manner.
4. Access to data should be restricted to those who **need** to use it for BC purposes.
5. All emails should include information on how to stop receiving or unsubscribe to email communications in the future.
6. Data should be kept up to date and destroyed when out of date or no longer needed.
7. You should ensure that permission has been given prior to contacting members by email.
8. Always ensure emails addresses are listed in the “bcc” line.
9. When sending personal data electronically to other committee members ensure it has been encrypted and password protected.
10. Notify Head Office (Catherine Levett) of any changes to member personal data held.

Please note this is a working document and will be updated and amended as and when required.

If you have a query or data protection issue which is not covered above please contact Sandra Muldoon at Head Office to discuss.

Branch agreement

We would be grateful if you could sign and return the attached agreement form to confirm your Branch will comply with the guidelines detailed in this document.

Please ensure that each and every Committee member who will have access to or will hold personal data in paper format or electronically has read and agreed to abide by these guidelines before you return the agreement form.

Once confirmation is received we will be able to provide your Membership Secretary with all email addresses held for your Branch members.

May 2011