

**Data Protection (GDPR) Policy**

| Audience: | All Audiences |
| --- | --- |
| Policy Owner: | Paris Carter (Membership Secretary and Data Protection Lead) |
| Review Delegation: | Board of Trustees (Committee Members) |
| Review Cycle: | Every 2 years |
| Last Review: | October 2024 |
| Due for Review: | October 2026 |
| Version Number: | v6.10.2024 |

**Contents**

| **Section** | **Page number(s)** |
| --- | --- |
| Who are we? | 3 |
| What is Data Protection? | 3 |
| What data is covered under Data Protection? | 3-4 |
| What about GDPR? | 4-5 |
| What are my responsibilities? | 5 |
| Who should I talk to for more information? | 5 |
| What do I do if I suspect data has been lost, accessed inappropriately or there has been a data breach? | 5-6 |
| What if I want to raise a complaint? | 6 |
| How long is personal data retained? | 6-7 |
| Glossary of terms | 7 |

1. Who are we?

The Hampshire Bat Group (“HBG”) is a registered charity in England and Wales (1095874). HBG is committed to protecting personal data in a manner that respects individual rights while enabling the group to continue working to protect bats. This Data Protection (GDPR) Policy will outline how we look after and process personal data and how the law protects individuals.

Data Protection Lead (as of April 2024):

Paris Carter - [dataprotectionhantsbats@gmail.com](about:blank)

1. What is Data Protection?

Data protection is a series of laws, processes and policies that ensure organisations and individuals safeguard any and all personal data they hold and process.

Data protection laws only relate to data about a living individual.

The Data Protection Act (2018) covers 4 types of data:

1. Information processed, or intended to be processed by automatic means.

a. Generally, this is computer held data.

2. Information processed in a non-automated manner, which forms part of, or is intended to form part of a ‘filing system’.

a. Generally, this is a paper filling system.

3. Information that forms part of an ‘accessible record’

a. This is information such as health records etc. parts of which may be accessed by different organisations.

4. Information held by a public authority

a. This type of information is referred to as category E data.

Detailed information about data protection can be located on the Information Commissioner’s Office (ICO) website: [https://ico.org.uk/](about:blank)

1. What data is covered under Data Protection?

Data protection laws split our data between two main categories:

* Personal Data
* Special Category information

Personal data means any information relating to an identified or identifiable natural person (Data Subject).

The identifiable categories (specific to HBG) are:

* Name
* Membership Database Accession Number (Membership Number)
* Photos
* Address
* Email Address
* Telephone Numbers

Special Category data covers more sensitive data, such as:

* Race
* Ethnic Origin
* Political Opinions
* Religious or Philosophical Beliefs
* Genetic Data
* Health and Medical Data

1. What about GDPR?

General Data Protection Regulation (GDPR) is an additional set of laws, processes and procedures, that came into effect in May 2018. GDPR advances and updates the Data Protection Act (2018) but does not replace it.

GDPR focuses more on the protection of the data subjects and clears up grey areas surrounding the use of digital media.

The eight main focuses and rights of GDPR, in summary, are:

1. The right to be informed

* This is about providing individuals with clear and concise information about what we do with their personal data, including how we collect data, our purposes for processing data, data retention periods and who data will be shared with.

2. The right of access

* This gives individuals the right to obtain a copy of their personal data, which helps individuals to understand how and why we are using their data

3. The right to rectification

* Individuals have the right to have personal data rectified if it is inaccurate or incomplete without undue delay

4. The right to erasure

* Individuals have the right, in certain circumstances, to ask for their personal data to be deleted without undue delay. For example, where it is no longer necessary for the organisation to hold the data about an individual or individuals have withdrawn their consent to process or store their data. If organisations are unable to comply with an erasure request, they must explain this to the individual in their response.

5. The right to restrict processing

* Individuals have the right to restrict the processing of their personal data in certain circumstances, for example they have issues with the content of the information an organisation holds or how the organisation has processed their data.

6. The right of data portability

* This allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

7. The right to object

* An individual can object to the processing of their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing. This is an absolute right and there are no exemptions or grounds for organisation’s to refuse.

8. Rights in relation to automated decision making

* Individuals have the right to not be subject to a decision based solely on automated processing. Processing is “automated” where it is carried out without human intervention and where it produces legal effects or significantly affects an individual. Automated processing includes profiling. HBG does not utilise automated decision making.

1. What are my responsibilities?

All members within the Group have a responsibility to look after and maintain any data they have access to. Data relating to our members (current, past or prospective) must be treated with respect and be processed in line with our legal obligations. Data must only be processed if there is a justifiable reason.

One of the most significant data breach risks is with paper based data. If you have printed any paperwork that contains personal or special category data, then it is your responsibility to ensure the paper:

1. Cannot be accessed by anyone who should not have access to it

2. Is stored safely and securely

3. Is destroyed correctly

1. Who should I talk to for more information?

If you need any further information, then please contact the Data Protection Lead at [dataprotectionhantsbats@gmail.com](about:blank)

1. What do I do if I suspect data has been lost, accessed inappropriately or there has been a data breach?

If you suspect there has been any data lost, accessed inappropriately or has been a data breach that contains any of the categories under data protection, then it is important to notify us as quickly as you can.

In the first instance, you must always contact the Data Protection Lead via email at [dataprotectionhantsbats@gmail.com](about:blank) (please include ‘**URGENT - DPL**’ in the email subject line) who will provide further advice and guidance.

Once notification has been made the following process will be followed:

**STAGE 1 - DISCOVERY**

Step 1: Breach discovery

Step 2: Contact the Data Protection Lead via email as soon as possible after the incident/breach at [dataprotectionhantsbats@gmail.com](about:blank) and include ‘**URGENT - DPL**’ in the email subject line

**STAGE 2 - INITIAL ASSESSMENT**

Step 1: Initial investigation by Data Protection Lead within 24 hours, where possible

Step 2: Breach Severity Assessment conducted by the Data Protection Lead within 48 hours, where possible, of the breach. This is partly completed through the Information Commissioner’s Office ‘Self Assessment for Data Breaches’ tool that is available on their website: [https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/](about:blank)

Step 3: Plan of Action provided by the Data Protection Lead within 72 hours, where possible

**STAGE 3 - NOTIFICATION**

Step 1: Reportable data breaches must be made to the Information Commissioner's Office within 72 hours after being made aware of the breach, with any delay beyond this requiring justification. This is completed through the online form available through the Information Commissioner’s Office website: [https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/report-a-data-breach-online-form/](about:blank)

Step 2: Notify affected individuals within 96 hours of being made aware of the breach

Step 3: Notify any relevant Third Parties within 120 hours of being made aware of the breach

**STAGE 4 - RESPONSE**

Step 1: Update Information Commissioner's Office as required/requested

Step 2: Evaluation and response to be presented by Data Protection Lead to the Board of Trustees (Committee Members)

1. What if I want to raise a complaint?

If you have a complaint, in the first instance, please contact the Data Protection Lead at [dataprotectionhantsbats@gmail.com](about:blank) so we can try to address and resolve your concerns.

If the Data Protection Lead has not resolved your concern satisfactorily or within a reasonable time frame, you can raise your concern directly to the Information Commissioner's Office - [https://ico.org.uk/global/contact-us/contact-us-public/](about:blank) - or via phone 0303 123 1113.

1. How long is personal data retained?

Personal data - which includes electronic and paper based data - for our members is stored, maintained and processed for the duration of an active membership subscription, plus one month after the subscription has ended or lapsed.

The Group has produced an ‘Article 30’ document which outlines the Group’s processing activities and includes details such as what categories of data we hold, what measures we have in place to secure data and more. This is available to view upon request.

1. Glossary of terms

* GDPR – General Data Protection Regulation
* HBG – Hampshire Bat Group
* Board of Trustees - this includes the Chair, Membership Secretary, Treasurer, County Recorder, Committee Secretary and other select individuals
* Data Protection laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including, in the UK, the Data Protection Act 2018.
* Data Protection Lead – an individual who assists the organisation to monitor internal compliance, inform and advise on the organisation’s data protection obligations and act as a contact point for data subjects and the Information Commissioner.
* ICO – the Information Commissioner’s Office, the UK’s independent data protection regulator
* Personal data – Any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.
* Processing – Any collection, use or storage of Personal Data whether on the Group’s information systems or in paper form.
* Special Categories of Personal Data - Personal Data that reveals a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.