DATA PROTECTION POLICY

You must read this policy because it gives important information about:

- the data protection principles with which the Company must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, eg about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached copy to the data protection officer finance@themammalsociety.org.

1 Introduction

1.1 The Company obtains, keeps and uses personal information (also referred to as data) about job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices for a number specific lawful purposes, as set out in the Company's data access request policy.

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce, and how (and when) we delete that information once it is no longer required.

1.4 The Company's data protection officer, Janet Pressland, is responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer finance@themammalsociety.org OR the Chair of the Mammal Society.

1.5

2 Scope

2.1 This policy applies to the personal information of job applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

2.2 Staff should refer to the Company's data subject access request policy and, where appropriate, to its other relevant policies including in relation to criminal record information which contain further information regarding the protection of personal information in those contexts.

2.3 We will review and update this policy in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

3 Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4 Data protection principles

4.1 The Company will comply with the following data protection principles when processing personal information:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;

4.1.5 we will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal information

5.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, ie:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

(f) that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 5.2 below.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie that there is no other reasonable way to achieve that purpose);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

5.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 6.2.2 below), and document it; and

5.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

5.2 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

5.2.3 keep the LIA under review, and repeat it if circumstances change; and

5.2.4 include information about our legitimate interests in our relevant privacy notice(s).

6 Sensitive personal information

6.1 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

6.2 The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

6.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above, eg it is necessary for the performance of the employment contract, to comply with the Company's legal obligations or for the purposes of the Company's legitimate interests; and

6.2.2 one of the special conditions for processing sensitive personal information applies, eg:

(a) the data subject has given has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

6.3 Before processing any sensitive personal information, staff must notify the data protection officer of the proposed processing, in order that the data protection officer may assess whether the processing complies with the criteria noted above.

6.4 Sensitive personal information will not be processed until:

6.4.1 the assessment referred to in paragraph 6.3 has taken place; and

6.4.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.5 The Company's data access request notice sets out the types of sensitive personal information that the Company processes, what it is used for and the lawful basis for the processing.

6.6 In relation to sensitive personal information, the Company will comply with the procedures set out in paragraphs 6.8 and 6.9 below to make sure that it complies with the data protection principles set out in paragraph 4 above.

6.7 **During the recruitment process**: the panel, with guidance from the data protection officer OR Chair of the Society, will ensure that (except where the law permits otherwise):

6.7.1 during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, eg race or ethnic origin, trade union membership or health;

6.7.2 if sensitive personal information is received, eg the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

6.7.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

6.7.4 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

6.7.5 we will only ask health questions once an offer of employment has been made.

6.8 **During employment**: the finance department, with guidance from the Chair, will process:

6.8.1 health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

6.8.2 sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting; and

6.8.3 trade union membership information for the purposes of staff administration and administering 'check off'.

7 Criminal records information

Criminal records information will be processed in accordance with the Company's Criminal Records Policy.

8 Data protection impact assessments (DPIAs)

8.1 Where processing is likely to result in a high risk to an individual's data protection rights (eg where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

8.1.1 whether the processing is necessary and proportionate in relation to its purpose;

8.1.2 the risks to individuals; and

8.1.3 what measures can be put in place to address those risks and protect personal information.

8.2 Before any new form of technology is introduced, the manager responsible should therefore contact data protection officer in order that a DPIA can be carried out.

8.3 During the course of any DPIA, the employer will seek the advice of the data protection officer.

9 Documentation and records

9.1 We will keep written records of processing activities which are high risk, ie which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

9.1.1 the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);

9.1.2 the purposes of the processing;

9.1.3 a description of the categories of individuals and categories of personal data;

9.1.4 categories of recipients of personal data;

9.1.5 where possible, retention schedules; and

9.1.6 where possible, a description of technical and organisational security measures.

9.2 As part of our record of processing activities we document, or link to documentation, on:

9.2.1 information required for privacy notices;

9.2.2 records of consent;

9.2.3 controller-processor contracts;

9.2.4 the location of personal information;

9.2.5 DPIAs; and

9.2.6 records of data breaches.

9.3 If we process sensitive personal information or criminal records information, we will keep written records of:

9.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

9.3.2 the lawful basis for our processing; and

9.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

9.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

9.4.1 carrying out information audits to find out what personal information the Company holds;

9.4.2 distributing questionnaires and talking to staff across the Company to get a more complete picture of our processing activities; and

9.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

10 Privacy notice

10.1 The Company will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

10.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

11 Individual rights

11.1 You (in common with other data subjects) have the following rights in relation to your personal information:

11.1.1 to be informed about how, why and on what basis that information is processed

11.1.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see the Company's subject access request policy;

11.1.3 to have data corrected if it is inaccurate or incomplete;

11.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

11.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

11.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

11.2 If you wish to exercise any of the rights in paragraphs 11.1.3 to 11.1.6, please contact the data protection officer.

12 Individual obligations

12.1 Individuals are responsible for helping the Company keep their personal information up to date. You should let finance department know if the information you have provided to the Company changes, for example if you move house or change details of the bank or building society account to which you are paid.

12.2 You may have access to the personal information of other members of staff, suppliers and customers of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 11.1 above.

12.3 If you have access to personal information, you must:

12.3.1 only access the personal information that you have authority to access, and only for authorised purposes;

12.3.2 only allow other Company staff to access personal information if they have appropriate authorisation;

12.3.3 only allow individuals who are not Company staff to access personal information if you have specific authority to do so from data protection officer;

12.3.4 keep personal information secure (eg by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's Staff Handbook);

12.3.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

12.3.6 not store personal information on local drives or on personal devices that are used for work purposes.

12.4 You should contact the data protection officer or Chair if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.4.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 6.2.2 being met;

12.4.2 any data breach as set out in paragraph 15.1 below;

12.4.3 access to personal information without the proper authorisation;

12.4.4 personal information not kept or deleted securely;

12.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures being in place;

12.4.6 any other breach of this Policy or of any of the data protection principles set out in paragraph 4.1 above.

13 Information security

13.1 The Company will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

13.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;

13.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

13.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

13.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

13.2 Where the Company uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

13.2.1 the organisation may act only on the written instructions of the Company;

13.2.2 those processing the data are subject to a duty of confidence;

13.2.3 appropriate measures are taken to ensure the security of processing;

13.2.4 sub-contractors are only engaged with the prior consent of the Company and under a written contract;

13.2.5 the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights under the GDPR;

13.2.6 the organisation will assist the Company in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

13.2.7 the organisation will delete or return all personal information to the Company as requested at the end of the contract; and

13.2.8 the organisation will submit to audits and inspections, provide the Company with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Company immediately if it is asked to do something infringing data protection law.

13.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the **[**data protection officer OR [*insert job title or department*]**]**.

14 Storage and retention of personal information

14.1 Personal information (and sensitive personal information) will be kept securely.

14.2 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Where there is any uncertainty, staff should consult the data protection officer.

14.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

15 Data breaches

15.1 A data breach may take many different forms, for example:

15.1.1 loss or theft of data or equipment on which personal information is stored;

15.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

15.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

15.1.4 human error, such as accidental deletion or alteration of data;

15.1.5 unforeseen circumstances, such as a fire or flood;

15.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

15.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

15.2 The Company will:

15.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

15.2.2 notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

16 International transfers

16.1 The Company may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to the USA and Canada on the basis that that country, territory or organisation is designated as having an adequate level of protection.

17 Training

The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

18 Consequences of failing to comply

18.1 The Company takes compliance with this policy very seriously. Failure to comply with the policy:

18.1.1 puts at risk the individuals whose personal information is being processed; and

18.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and

18.1.3 may, in some circumstances, amount to a criminal offence by the individual.

18.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

18.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection officer.

I have read and understood this policy and agree to abide by its terms.

Signed.....