BRITISH ACADEMY OF FORENSIC SCIENCES

Data Retention Policy

1. **Introduction**

This Policy sets out the obligations of British Academy of Forensic Sciences, ("the Charity") a Charity registered in the UK under the charity number 299875 whose registered office King's College London, 150 Stamford Street, London, SE1 9NH regarding retention of personal data collected, held, and processed by the Charity in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for **no longer than is necessary for the purposes for which the personal data is processed**. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and the Charity has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation; or

f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Charity for the investigation of alleged miscarriages of justice purposes and the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Charity complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Charity, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by the Charity **and** any Third-Party suppliers processing personal data on the Charity's behalf.

3.2 Personal data, as held by the Charity or the above is stored in the following ways and in the following locations:

a) The Charity's secure servers, located in Cloud secure storage.

b) Computers permanently located in the Charity's premises.

c) Computers and mobile devices owned by managers, trustees, employees, agents, and sub-contractors and used in accordance with the Charity's Data Protection Agreements.

d) Physical records

4. Data Subject Rights and Data Integrity

All personal data held by the Charity is held in accordance with the requirements of the GDPR and data subjects' rights thereunder,

4.1 Data subjects are kept fully informed of their rights, of what personal data the Charity holds about them, how that personal data is used and how long the Charity will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.2 Data subjects are given control over their personal data held by the Charity including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Charity's use of their personal data and further rights relating to automated decision-making and profiling. British Academy of Forensic Sciences as a Charity does not use or adopt automated decision-making and profiling.

5. Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within the Charity to protect the security of personal data.

a) All emails containing personal data must be encrypted;

b) All emails containing personal data must be marked "confidential";

c) Personal data may only be transmitted over secure networks;

d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using an approved and authorised secure courier company, the recipient should be informed in advance and should be waiting to receive it, and the delivery should be signed for.

h) All personal data transferred physically should be transferred in a suitable container marked “confidential”;

i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from either the Secretary General or Administrator.

j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Charity or not, without authorisation;

l) Personal data must be handled with care at all times and should not be left unattended or on view;

m) Computers used to view personal data must always be locked before being left unattended;

n) No personal data should be stored on any mobile device, whether such device belongs to the Charity or otherwise, without the formal written approval of the Secretary General and/or Administrator and then strictly in accordance with all instructions and limitations described at the time the approval is

given, and for no longer than is absolutely necessary**;**

o) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Charity where the party in question has agreed to comply fully with the Charity's Data Protection Policy and the GDPR;

p) All personal data stored electronically should be backed up regularly with backups stored in our Secure Cloud. All backups should be encrypted;

q) All electronic copies of personal data should be stored securely using passwords and encryption;

r) All passwords used to protect personal data should be changed regularly and must be secure;

s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

t) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

u) No software may be installed on any Charity-owned computer or device without approval; and

v) Where personal data held by the Charity is used for marketing purposes, it shall be the responsibility of the Secretary General and/or Administrator to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

The following organisational measures are in place within the Charity to protect the security of personal data.

a) All employees and other parties working on behalf of the Charity shall be made fully aware of both their individual responsibilities and the Charity's responsibilities under the GDPR and under the Charity's Data Protection Policy;

b) Only employees and other parties working on behalf of the Charity that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Charity;

c) All employees and other parties working on behalf of the Charity handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Charity handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Charity handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) The performance of those employees and other parties working on behalf of the Charity handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Charity handling personal data will be bound by contract to comply with the GDPR and the Charity's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of the Charity handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Charity arising out of the GDPR and the Charity's Data Protection Policy;

6. Data Disposal

Upon the expiry of the data retention periods set out below in **Part 7** of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data (contact details only) stored electronically (including any and all backups thereof) shall be deleted electronically**.**

6.2 Special category personal data, such as legal case files, court papers and expert reports stored electronically (including any and all backups thereof) shall be deleted electronically.

6.3 Personal data stored in hardcopy form shall be shredded to Level 3 standard by an approved contractor or an appropriate level shredding machine.

7. Data Retention

7.1 As stated above, and as required by law, the Charity shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Charity;

b) The type of personal data in question;

c) The purpose(s) for which the data in question is collected, held, and processed;

d) The Charity's legal basis for collecting, holding, and processing that data;

e) The category or categories of data subject to whom the data relates;

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data, including papers that have been sent to us by a data subject about their case, may be deleted or otherwise disposed of prior to the expiry of its

defined retention period where a decision is made within the Charity to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR. Our Data and Retention periods are as follows:

Data Ref.	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Name	Personal	Communication	1 year	1 year	Retained upon membership renewal for a further 12 months
Address	Personal	Communication	1 year	1 year	Retained upon membership renewal for a further 12 months
Gender	Personal	Communication	1 year	1 year	Retained upon membership renewal for a further 12 months
Email address	Personal	Communication	1 year	1 year	Retained upon membership renewal for a further 12 months
Telephone number	Personal	Communication	1 year	1 year	Retained upon membership renewal for a further 12 months
Payment Information	Personal	Membership Payments	1 year	1 year	Retained upon membership renewal for a further 12 months

8. Roles and Responsibilities

8.1 The Secretary General and/or Administrator shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Charity's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.2 The Secretary General and/or Administrator shall be directly responsible for ensuring compliance with the above data retention periods throughout the Charity.

8.3 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to contact@bafs.org.uk

9. Implementation of Policy

This Policy shall be deemed effective as of 01.01.2022. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Tracy Alexander

Position: President of the British Academy of Forensic Sciences

Date: 1st November 2022

Due for Review by: 31st October 2024

Signature: