THE CRIMINAL BAR ASSOCIATION

GOVERNANCE PAPER

Information Governance Policy

1. Purpose and Scope

1.1 This Policy governs the handling of personal data, governance records, operational information and digital systems by the Criminal Bar Association ("the Association").

1.2 It gives effect to:

(a) the obligations of the Association under the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018;

(b) Part 13 of the Constitution (Records, Property and Intellectual Property);

(c) Part 5 of the Constitution (Administration and Operations) in respect of operational systems;

(d) clause 3.6 and clause 3.11 of the Constitution in respect of digital access by membership category;

(e) the data retention requirements of the Election Procedures and the Complaints, Conduct and Behaviour Policy.

1.3 This Policy applies to all personal data and governance records held by the Association, in any form (electronic or paper).

2. Roles and Responsibilities

2.1 The Association is the data controller in respect of personal data which it determines the purposes and means of processing.

2.2 The Administrator has operational responsibility for information governance under this Policy and acts as the principal point of contact for data protection matters, reporting to the Chair and Vice Chair, in accordance with clause 5.4 of the Constitution.

2.3 The Officers have collective oversight of information governance and shall consider information governance matters at the Executive Committee not less than annually.

2.4 Where the Administrator processes personal data on behalf of the Association as a self-employed contractor, the Administrator does so as a data processor on the terms of the Engagement Letter and the data processing schedule appended to it.

3. Data Protection Principles

3.1 In handling personal data the Association shall:

(a) process personal data lawfully, fairly and transparently;

(b) collect and process personal data only for specified, explicit and legitimate purposes;

(c) process personal data only to the extent necessary for those purposes (data minimisation);

(d) take reasonable steps to keep personal data accurate and up to date;

(e) retain personal data only for so long as is reasonably necessary;

(f) process personal data securely, with appropriate technical and organisational measures.

4. Categories of Personal Data Held

4.1 The Association ordinarily holds personal data in the following categories:

(a) membership data — names, contact details, professional information (chambers, year of call, practice area), membership category, subscription status;

(b) event and engagement data — attendance records, event registration information, communications preferences;

(c) governance data — records of declared interests, attendance at Executive Committee and Subcommittee meetings, records of those holding office;

(d) communications data — podcast subscriber data, mailing list data, engagement metrics;

(e) complaints and welfare data — confidential records under the Complaints, Conduct and Behaviour Policy and the Wellbeing Framework, which constitute special category data where they reveal health, religious belief, sexual life or other protected categories;

(f) financial data — in respect of subscriptions, expenses, contracts and bursary applications.

5. Lawful Bases for Processing

5.1 The Association relies on the following lawful bases for processing under Article 6 of the UK GDPR:

(a) legitimate interests, in respect of membership administration, governance, communications with members, and the operational running of the Association;

(b) consent, where required (in particular for marketing communications and for the publication of personal information about members);

(c) contract, in respect of payments, subscriptions, engagements with contractors, and event participation;

(d) legal obligation, where required by law.

5.2 In respect of special category data, the Association relies on Article 9 of the UK GDPR, in particular explicit consent, the substantial public interest, and the purposes of preventive medicine and occupational welfare in respect of wellbeing matters.

6. Data Subject Rights

6.1 Members and other data subjects have the rights conferred by the UK GDPR, including:

(a) the right of access to their personal data;

(b) the right to rectification of inaccurate data;

(c) the right to erasure in certain circumstances;

(d) the right to restriction of processing in certain circumstances;

(e) the right to data portability where applicable;

(f) the right to object to processing on certain grounds;

(g) the right to lodge a complaint with the Information Commissioner’s Office.

6.2 Requests to exercise data subject rights shall be addressed to the Administrator. The Association shall respond within one month of receipt, save where an extension is permitted by the UK GDPR.

7. Sharing and Disclosure

7.1 Personal data shall not be shared with third parties save:

(a) with service providers acting as data processors on behalf of the Association under appropriate contractual terms;

(b) as required by law or by a regulatory body of competent jurisdiction;

(c) with the consent of the data subject;

(d) where strictly necessary for the legitimate operation of the Association (such as the sharing of attendance lists with venue providers).

7.2 Member contact lists shall not be made available to candidates in any election (governed by Section 11 of the Election Procedures), to commercial third parties, or for political purposes.

8. Security and Systems

8.1 The Association shall maintain appropriate technical and organisational measures to protect personal data, including:

(a) access controls (multi-factor authentication where reasonably available);

(b) encryption of data in transit and, where reasonably practicable, at rest;

(c) segregation of operational systems by membership category in accordance with clauses 3.6 and 3.11 of the Constitution;

(d) secure backups;

(e) incident response procedures.

8.2 Operational systems maintained at the expense of the Association remain the property of the Association in accordance with clause 5.6 of the Constitution. Where operational infrastructure utilised by the Association is personally owned, funded, licensed or maintained by an authorised individual, ownership remains with that individual in accordance with clause 5.7 of the Constitution. The arrangements covering the Association's digital estate are set out in the Digital Estate Terms of Engagement.

8.3 The Administrator shall maintain a record of the systems used in the Association's operations, including those personally owned, those owned by the Association, and those provided by third-party service providers.

9. Records Retention

9.1 Records shall be retained only for so long as is reasonably necessary having regard to:

(a) the purposes for which the data was collected;

(b) any legal or regulatory retention requirements;

(c) the legitimate interests of the Association in maintaining institutional memory.

9.2 The Association adopts the following standard retention periods, save where particular circumstances justify a different period:

(a) membership records — duration of membership, plus six years;

(b) governance records (minutes, agendas, papers) — indefinite, as part of the Association's historical archive;

(c) financial records — seven years (in accordance with HMRC requirements);

(d) election records — not less than six years;

(e) complaints and conduct records — six years from final outcome, save where longer retention is required;

(f) wellbeing referrals and welfare records — retained only with the consent of the individual concerned, and otherwise for the minimum period necessary;

(g) event and engagement records — three years;

(h) marketing communications data — only for so long as consent is current.

9.3 The Administrator shall conduct an annual records review and shall securely dispose of records no longer required.

10. Digital Access and Permissions

10.1 Access to digital systems, applications, platforms and member services operated by the Association shall be allocated by reference to operational need and to membership category, in accordance with clause 3.11 of the Constitution and policies approved by the Officers.

10.2 Student Members shall not have access to member-only digital applications or operational systems of the Association, in accordance with clause 3.6 of the Constitution.

10.3 Honorary Members shall be granted such digital access as the Officers consider appropriate.

10.4 Officers and members of the Executive Committee shall have access appropriate to their role.

10.5 Access for Subcommittee members and Working Group members shall be granted by the Administrator on the instruction of the relevant Subcommittee Chair or Working Group Chair.

10.6 Access shall be reviewed periodically and shall be removed promptly on the cessation of role or membership.

10.7 Access may be restricted, suspended or removed by the Officers where there is reason to believe that access has been or is being misused.

11. Data Breach

11.1 A personal data breach shall be reported to the Administrator without delay on becoming aware of it.

11.2 The Administrator, in consultation with the Officers, shall:

(a) assess the breach and the risk it presents;

(b) take steps to contain the breach;

(c) where the breach is likely to result in a risk to the rights and freedoms of natural persons, notify the Information Commissioner’s Office without undue delay and where feasible within seventy-two hours;

(d) where the breach is likely to result in a high risk to the rights and freedoms of natural persons, notify the data subjects affected without undue delay;

(e) maintain a record of the breach and the response.

12. Members’ Privacy Notice

12.1 The Association shall maintain a privacy notice on its website setting out, in plain language, how it handles personal data, the lawful bases on which it relies, and the rights of data subjects. 12.2 The privacy notice shall be reviewed annually by the Administrator and approved by the Officers.

13. Review

13.1 This Policy shall be reviewed by the Executive Committee not less frequently than every two years.

/