Data-sharing protocol for the sharing and disclosure of information between

The Council of the Inns of Court (BTAS and the ICC)

And

The Honourable Society of The Inner Temple

And

The Honourable Society of The Middle Temple

And

The Honourable Society of Gray's Inn

And

The Honourable Society of Lincoln's Inn

Purpose

1. This document ('the Protocol') provides a framework for the collection, sharing, retention and destruction of information between the independent data controllers ('the parties'); the Council of the Inns of Court (COIC) through its disciplinary bodies and the four Inns of Court: Inner Temple, Middle Temple, Gray's Inn and Lincoln's Inn.

2. It provides a guide for members of the four Inns of Court about how their data might be shared amongst the Inns and with COIC (and vice versa), what data might be shared and the reason for the sharing. This protocol does not cover the relationship the Inns have with the ICCA as an authorised training organisation.

3. This protocol should be read in conjunction with the data protection policy and privacy notices of the Inns of Court and COIC. These can be found on the Inns' and COIC's websites as below. Insert hyperlinks to privacy statements here.

4. The sharing of personal data set out in this protocol is necessary to ensure that the Inns of Court have adequate regulatory oversight of their students, and that the responsibilities of COIC and the Inns, as set out in the Memorandum of Understanding with the Bar Standards Board, and the Inns' policies are complied with and that jointly held events and training are organised effectively.

Definitions

COIC – means the Council of the Inns of Court and includes the Inns' Conduct Committee and the Bar Tribunals and Adjudication Service.

Inns of Court – means each of the four Inns of Court; the Honourable Society of The Inner Temple, the Honourable Society of The Middle Temple, the Honourable Society of Gray's Inn and the Honourable Society of Lincoln's Inn.

Party – means one of COIC or the Inns

Parties – means more than one Party

Data controller – means a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any shared personal data is processed

Data Processor in relation to shared personal data – means any person (other than an employee of the data controller) who processes the shared personal data on behalf of the data controller

Data Protection Officer – referred to as DPO throughout the document means the nominated individual within each party who oversees the party's processing of personal data and ensures it is complying with its data protection obligations under the Data Protection Legislation, including the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

Memorandum of Understanding – means the document agreed between the BSB, COIC and the four Inns of Court in relation to education and training for the Bar.

Processing – means any operation or set of operations which is performed on shared personal data or on sets of shared personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Shared Personal Data – The personal data to be shared between the parties under Annex 1 of this agreement. 'Personal data to be shared' will be construed accordingly.

Risk and Security

5. The process of transferring personal data includes a risk of security breaches. However, this is mitigated by the robust security policies and measures which each party has in place. There is also a risk that we do not use the shared personal data in line with the UKGDPR requirements. This risk is mitigated by the parties upholding this protocol, their own commitment to handling personal data and their obligations within the MOU between the Inns, COIC and the Bar Standards Board.

6. The parties acknowledge that there is a risk in sharing data, but all parties have robust data protection policies and security measures in place and take their responsibilities for the security of personal data very seriously. The parties are sure that individuals can have confidence in the measures put in place and that the Inns, and COIC, have instituted data protection by design and default.

7. The parties are also committed to upholding their responsibilities under this agreement, the MOU and the current data protection legislation.

8. The parties agree to act as independent data controllers in respect of the data shared between Inns.

9. Annex 2 sets out the individuals who are the nominated Data Protection Officers/Leads (DPO) and therefore have responsibility to ensure that only those who require access to the shared personal data can have this.

The data to be shared

10. The parties agree that the shared personal data set out in Annex 1 is the least amount of personal data required to be shared to ensure the Inn is assured that their regulatory and membership functions are administered satisfactorily. This also sets out the purpose for which the personal data is shared between the parties.

11. The shared personal data collected and stored by each party is set out in Annex 1 and should be used for the stated purposes only, and in accordance with relevant statutory, regulatory, and policy provisions.

12. The Parties agree to inform individuals who provide their data which is shared under this Protocol of the existence of this protocol through their Privacy Notices and Data Protection Policies.

Retention

13. The parties will only retain shared personal data for as long as is necessary for the legitimate purposes for which the shared personal data is processed (which may be different for each party). This period is determined by the party's own data protection and/or data retention policies. Where retention periods have been agreed by the parties for specific categories of data these are set out in Annex 1.

14. Each party is responsible for ensuring that when those legitimate purposes come to an end, the shared data is securely deleted.

15. The parties are each responsible for ensuring that the data they hold is held securely and in line with current best practice and that the data is secure by design and default.

The Rights of the Data Subject, Monitoring & Complaints

16. The Data Protection Act provides the following rights for the individual data subject:
    i. The right to be informed
    ii. The right of access
    iii. The right to rectification
    iv. The right to erasure
    v. The right to restrict processing
    vi. The right to data portability
    vii. The right to object
    viii. Rights in relation to automated decision making and profiling.

17. Any requests pertaining to objection to processing, rectification, erasure, restriction and portability should be dealt with by the party that the data subject provided their data to. That party should inform the other parties when that request impacts on data that has been shared with them.

18. Individuals wishing to submit a subject access request should do so to each organisation they are seeking personal data from.

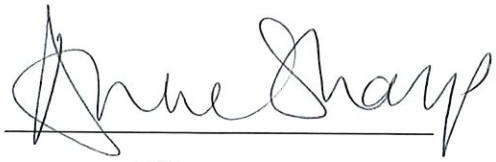
19. The parties sharing personal data will be responsible for monitoring that data and with which other parties it has been shared.

20. Any complaints about the way any of the parties have used personal data should in the first instance be directed to the parties' DPO.

21. The data subject also has the right to complain to the ICO if they are not satisfied with the way the parties use their information. The data subject can contact the ICO by writing to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Ad Hoc or one-off Data Sharing

22. It may sometimes be necessary for the parties to share data in a way not covered by this agreement. In this scenario the party will where possible inform the data subject about the processing, but it may be necessary to decide to share data quickly, in conditions of real urgency or in an emergency.

Signature 

Date 17 Jan 2024

Anne Sharp CBE

Under Treasurer of the Honourable Society of Lincoln's Inn

Signature 

Date 17/1/24

Greg Dorey CVO

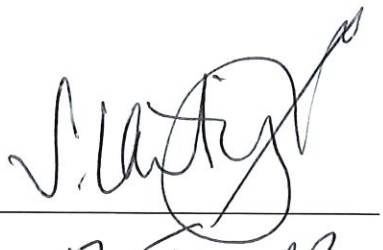
Sub-Treasurer of the Honourable Society of the Inner Temple

Signature 

Date 17/1/24

Sir Christopher Ghika KCVO CBE

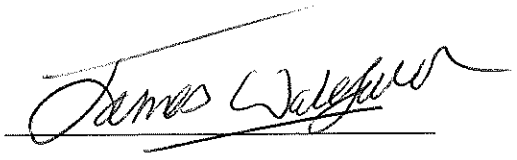
Under Treasurer of the Honourable Society of the Middle Temple

Signature 

Date 17 Jan 23

Brigadier Stephen Cartwright

Under Treasurer of the Honourable Society of Gray's Inn

Signature 

Date 17.1.24

James Wakefield KC (Hon)

Director of The Council of the Inns of Court

Annex 1 – the personal data to be shared

	The information to be shared	Purpose	Basis	How	When	Retention
1	**Scholarships Data**					
2	**Applicants for Scholarships**					
3	• Full names Secondary data i.e. date of birth may be shared in the case of applicants sharing first and second names.	To check that applicants for scholarships have only applied to one Inn (applying to more than one Inn is not permitted).	Legitimate interest	Password protected document from each Inn to the other Inns. Details of the mechanism used for the password protection of documents can be found at Annex 3.	Shortly after the deadline for applications has passed.	Deleted immediately after use.
4	**Disciplinary Data**					
5	In all disciplinary scenarios set out below any data shared by the Inns with BTAS will be provided in password protected documents. This Data Sharing Protocol sets out how the data is processed after it is received at BTAS. Each Inn's individual data processing policy will set out how this data will be processed within the Inn.					
6	**Applicants for admission to an Inn who withdraw their application before admission having declared matters.**					
7	• Name of applicant • Date of Birth • The category of matters declared (i.e. which question on the admission declaration they made a declaration under, but not the details of the declaration) or nature of	To prevent applicants who have withdrawn an application after declaring matters which call into question whether they are Fit and Proper, or	Task in the public interest	Password protected document from each Inn to the other Inns.	After withdrawal of application.	To be kept by the 4 Inns in line with their individual retention policies which would ordinarily be for the assumed

	The information to be shared	Purpose	Basis	How	When	Retention
	report (i.e. what type of institution a report has been received from e.g. academic institution).	after information about them has become known to the Inn, applying to another Inn without making a full disclosure.				lifetime of the applicant unless and until they have been admitted by an Inn of Court after being passed as Fit and Proper by the Inns' Conduct Committee, in which case the Inns apart from the Inn of admission will delete all data.
8	**Applicants for admission or student members whose referral to the ICC results in no sanction being imposed.**					
9	• Name • MyBar Number (if available) • Date of birth • Details of the disclosure or report which brought into question their status as Fit and Proper. • Result of the ICC proceedings.	To ensure that the Inn's records show that the applicant or Inn member is considered to be Fit and Proper.	Task in the public interest/legitimate interest	Password protected document from the ICC to the Inn concerned.	Within 7 days of the finding.	To be kept by the Inn concerned for the assumed lifetime of the applicant. COIC will dispose of the data 3 years after the appeal

	The information to be shared	Purpose	Basis	How	When	Retention
						period has expired.
10	**Applicants for Inn admission who are refused by the ICC.**					
11	• Name • Inn applied to • MyBar Number if available • Date of birth • Reason admission refused. • Time during which no further Inn application may be considered.	To ensure all Inns are aware that applications from the individual may not be considered for the time prescribed by COIC.	Task in the public interest	Password protected document from the ICC to the 4 Inns.	Within 7 days of the refusal being issued.	To be kept by the 4 Inns for the assumed lifetime of the applicant. Unless and until they have been admitted by an Inn of Court after being passed as Fit and Proper by the ICC, in which case the Inns apart from the Inn of admission will delete all data. COIC will dispose of the data 10 years after the appeal period has expired.
12	**Inn Members Suspended from or deprived of rights of membership of their Inn.**					

	The information to be shared	Purpose	Basis	How	When	Retention
13	• Name • Inn • Length of suspension or deprivation • Nature of suspension or deprivation. • Date of Birth • Date of Call	To prevent a suspended or deprived member exercising those rights they are prevented from using at another Inn of Court.	Legitimate interest	Password protected document from member's Inn to the other Inns.	When the rights of the member are deprived.	The Inn of Call will keep the data for the assumed lifetime of the applicant. The other Inns will keep the data for the length of the suspension or deprivation.
14	**Student Members having Call denied and being expelled from the Inn.**					
15	• Name • Inn • Inn membership number • Sanction imposed by the ICC • Date of Birth	To prevent a student applying to join another Inn without declaring they have previously been expelled from an Inn.	Task in the public interest	Password protected document from the ICC to the four Inns.	Within 7 days of the sanction being imposed.	To be kept by the 4 Inns for the assumed lifetime of the applicant. Unless and until they have been Called after being passed as Fit and Proper by the ICC in which case the Inns apart from the Inn of Call will delete all data.

	The information to be shared	Purpose	Basis	How	When	Retention
						COIC will dispose of the data 10 years after the appeal period has expired.
16	**Student Members having sanctions other than expulsion imposed by the ICC.**					
17	• Name • Inn • Inn membership number • Sanction imposed by the ICC	To enable Inns to keep the status of their members up to date. To enable Inns to appropriately schedule Call for members.	Task in the public interest	Password protected document from the ICC to the Inn of admission.	Within 7 days of the sanction being imposed.	The Inn of admission will keep the data for the assumed lifetime of the applicant. COIC will dispose of the data 6 years after the appeal period has expired.
18	**Called Members having been disbarred or suspended from practising at the Bar.**					
19	• Name • Inn • Inn membership number • Sanction imposed by BTAS • Date of Birth • Date of Call	To enable the Inns to keep the practising status of their members up to date. To prevent a suspended or disbarred member	Task in the public interest	In the case of disbarment: Password protected document from BTAS to the Inn of Call. In the case of suspension:	Within 7 days of the sanction being imposed.	In the case of disbarment the data will be kept by the Inn in line with their individual retention policies which would ordinarily

	The information to be shared	Purpose	Basis	How	When	Retention
		exercising those rights they are prevented from using.		Email from BTAS to the four Inns including the name of the member and a link to the BTAS website where the report relating to the finding is published.		be for the assumed lifetime of the applicant. In the case of suspension the data will be kept for the length of the suspension with the Inn of Call keeping the data in line with their individual retention policy which is expected to be for the lifetime of the applicant. BTAS will retain the data 'indefinitely' in the case of disbarment. In cases of suspension for more than a year they will dispose of the

	The information to be shared	Purpose	Basis	How	When	Retention
						data after 10 years. In cases of suspension for less than a year they will dispose of the data within 6 years.
20	Applicants who withdraw, are refused admission, are expelled or disbarred and then are subsequently admitted.					
21	• Name • Inn • Inn membership number if available. • MyBar Number if available. • Date of Birth • Call date if available.	To ensure Inns' records are correct.	Legitimate interest.	Password protected document from the relevant Inn to the other Inns.	Within 7 days of admission/readmission.	Deleted immediately after use.
22	**Event Data**					
23	**Event attendee details where two or more Inns are hosting a joint event or where one Inn is hosting but each Inn is taking bookings for their members.**					
24	• Name • Booking details (specific details to be determined by the host Inn). • Contact details • Dietary requirements	Ensure the smooth running of the event, that bookings are honoured and to ensure the health and safety of guests.	Contract	Password protected spreadsheet	Before the event.	In line with the Inns' own retention policies.
25	**Details of attendees at joint qualifying sessions**					

	The information to be shared	Purpose	Basis	How	When	Retention
26	• Name • Booking details (specific details to be determined by the host Inn). • Contact details • Dietary requirements	To ensure attendees receive the correct qualifying session 'points' for attending an event.	Contract	Password protected document from the hosting Inn to the other Inns.	Within 7 working days of the event.	In line with the Inns' own retention policies.
27	**Pupils' Advocacy Training**					
28	• Name • Inn • Whether the training has been successfully completed and any associated information.	To enable Inn membership records to show whether the person has successfully completed the training or if further training is needed when this training takes place at an Inn other than the Inn of Call.	Legitimate interest	Via email from the Inn holding the event to the other Inns who had members attend.	Within 7 working days of the event.	To be kept by the relevant Inns in line with their individual retention policies which would ordinarily be for the assumed lifetime of the member.
29	**Other**					
30	**Complaints and Subject Access Requests**					
31	• Name • Inn • MyBar Number	To enable responses to subject access requests and complaints to be	Legal obligation	By Email from the Inn receiving the request to those Inns with whom it has shared relevant data.	Within 7 working days of receipt of the subject access request/complaint.	Review every 2 years after last contact and delete if no longer relevant.

	The information to be shared	Purpose	Basis	How	When	Retention
		as complete as possible.				

Data Protection Officers (DPOs)

The DPOs are responsible for data protection compliance within their organisation. The DPOs are the designated contacts for subject access requests, queries, or complaints.

Party	Data Protection Officer
COIC	COIC Director James Wakefield (jwakefield@coic.org.uk / 0207 8220 761)
Inner Temple	Membership Registrar Jude Hodgson (Jhodgson@innertemple.org.uk / 020 7797 8206)
Middle Temple	Date Governance Manager Sarah Cates (s.cates@middletemple.org.uk / 0207 427 4809)
Gray's Inn	Director of Finance & Data Protection Officer Claire Johns (Claire.johns@graysinn.org.uk/ 0207 458 7803)
Lincoln's Inn	Data Protection Officer

	Naomi Johns (data.protection@lincolnsinn.org.uk / 0207 405 1393)

Annex 3

Transmitting and sending personal data

This protocol requires the sending of personal data to each organisation. This presents a risk to the subject in errors and accidents causing their personal data to be compromised.

Inn's staff who have responsibility for the administration of this protocol and the sharing of personal data will be required to read this guidance.

In sending personal data they should ensure that:

- The correct recipients address is in the TO line before pressing send.
- Personal data covered by this protocol should not be in the body of the email.
- No personal data should be in unprotected attachments.
- Personal data should be in password protected documents.
- Passwords should be sufficiently long and complex to prevent compromise.

When sending password protected documents by email Inn staff will advise the recipient in the body of the email to contact them via an alternative mechanism when they will be provided with the password for the document. The password must be kept securely.