Appendix I - Code Member Criteria & Requirements

The Code Member Criteria and requirements are set at a standard readily achievable by any business providing Code Services and represent the minimum requirement to achieve membership of the ABI and satisfy most Clients' expectations for their chosen provider of Code Services. However, Code Membership is available to any sector agency that meets the Code Member Criteria and requirements, whether a member of, or affiliated to, the ABI or not.

Code Member Criteria & requirements in detail		
All Code Members must satisfy requirements 1 to 14 set out below to the satisfaction of the Monitoring Body as detailed in paragraph 3.1 of the Code. **ABI Members will satisfy requirement 1 (i. to viii.) by virtue of their ABI membership.**		
Code Requirement		Supporting Evidence
1. At least one Principal of the Code Member's business must meet the criteria and provide the supporting evidence set out in this requirement.		An organogram or visual layout of the business structure showing persons in control, supported where relevant by up-to-date Companies House filings.
	i. Proof of identity and residential address.	Two certified forms of identity such as passport and driving licence and two proof of address documents such as a utility bill dated within the last three months.
	ii. Current professional indemnity insurance for the business with a minimum cover set at least £500,000.	A letter from the insurer confirming the required professional indemnity insurance cover is in place for the current period; OR any relevant certification of insurance.
	iii. ICO registration.	An up-to-date ICO registration certificate or a link to the ICO register with the correct contact and address details provided.

Code Member Criteria & requirements in detail		
	iv. A criminal conviction certificate (basic DBS disclosure) no older than 12 months for the first submission and no older than 3 years for each annual assessment.	A DBS application may be completed here https://www.gov.uk/request-copy-criminal-record.
	v. Two satisfactory professional or character references.	References to include work ethic, skills, strengths, and achievements and must include an endorsement of the applicant Code Member's honesty and suitability for Code Membership.
	vi. A comprehensive CV.	The CV must cover all qualifications, education and relevant work experience.
	vii. A personal and corporate financial probity check that is free of monetary judgments or insolvency. Any unsatisfied monetary judgments, undischarged insolvency, including debt relief order will disqualify from Code Membership.	A financial probity check can be completed through a variety of providers.
	viii. Work samples in the area of Code Services.	Two reports of work in the area of Code Services from the last two years with all Personal Data redacted. The cases reported must demonstrate the applicant Code Member's ability to communicate the outcomes of Code Services undertaken clearly and in a logical and orderly format.
2.Training	Adequate training and competence in Code Services and sector specific Data Protection Law requirements.	Satisfactory completion of data protection training to the level comparable to the ABI UK GDPR compliance workshop, or training to an equivalent standard on the areas covered by the Code, undertaken up to 12 months prior to application, and thereafter, every 3 years.

Code Member Criteria & requirements in detail		
		The MB may in its discretion consider other relevant and suitable qualifications.
	Maintenance of an adequate record of training completion and performance.	An up-to-date log of training completed, and scores achieved on any assessments undertaken. Evidence of course attendance or qualification certificate.
	Analysis of training needs to ensure that training provided is fit for purpose.	Evidence of usage of ABI comparable training modules to ensure that training covers the key areas of the Code.
	Training on roles and responsibilities.	Evidence of training addressing the differences between the roles of Controller, Joint Controller and Processor. A training requirement must be the Code Member assessing and explaining which role is undertaken in relation to hypothetical activities, and of the nature of the hypothetical processing under consideration.
	Training on DPIAs.	Evidence of training covering the requirements of Article 35 of the UK GDPR including: (i) carrying out a DPIA prior to processing commencing; and (ii) ensuring that a DPIA contains a description of processing, the necessity and proportionality of processing, an assessment of the risks to the rights and freedoms of Individuals and measures envisaged to address risks.
	Training on the lawful bases under Article 6 of the UK GDPR.	Evidence of training covering each of the lawful bases, when processing is necessary, why lawful bases for processing are important, how to decide which lawful basis applies, how to document the lawful basis and

Code Member Criteria & requirements in detail		
		what information needs to be provided to Individuals.
	Training on LIAs	Evidence of training covering completion of an LIA, when an LIA is required, assessment of the processing to decide on the outcome of an LIA, next steps after completion of the LIA and how LIAs overlap with DPIAs.
	Training on the seven Data Protection Principles.	Evidence of training outlining the seven Data Protection Principles under the UK GDPR and why the principles are important in the context of Code Services.
3. Legislative compliance	A legislation declaration confirming the Code Member's compliance with applicable legislation.	Code Members must review all relevant aspects of applicable legislation before making the legislation declaration. The declaration wording will be provided by the MB.
4.Roles and Responsibilities	The Code Member understands its role and responsibilities and documents and communicates them to its Clients accordingly. Code Members must understand the roles and responsibilities in respect of the data processing which they undertake. In accordance with Data Protection Law, and using the guidance in the Code, a Code Member must be able to establish if it is acting as a Processor, Controller, or a Joint Controller in relation to specific data processing.	Evidence (at the discretion of the MB) that the Code Member has documented and communicated to its Client the roles and responsibilities in respect of the data processing undertaken in the delivery of Code Services. This could be evidenced for example by providing a copy of the Client engagement letter and/or contract.
5. Case Extracts - DPIAs	Code Members must be able to determine when a DPIA is required and understand how to carry out the assessment.	A sample of up to three DPIAs which reflect the Code Member's range of services, redacted and anonymised, from live cases conducted by the Code Member during the previous 12 months. Or the review of a pre-existing DPIA, as required by the MB. The

Code Member Criteria & requirements in detail		
		DPIAs provided must be fully up to date and compliant with the requirements of Article 35 of the UK GDPR. The MB will take into consideration that the business may not regularly carry out DPIAs.
6. Case Extracts – Lawful Basis	Code Members, where necessary, must establish and appropriately document a lawful basis for data processing under Article 6 (and, where necessary, a condition under Article 9 or 10) of the UK GDPR, having considered the obligation under Article 5 of the UK GDPR for the Personal Data to be processed lawfully, fairly and in a transparent manner.	Case extracts, with an outline of the lawful basis relied on for the processing under Article 6, 9 and / or 10 of the UK GDPR and which demonstrates that the Code Member has considered its obligations under Article 5. Code Members must include evidence confirming that: (i) the purposes of processing activities have been reviewed and the most appropriate lawful basis has been chosen; (ii) the processing is necessary for the relevant purpose, and they are satisfied that there is no other reasonable and less-intrusive way to achieve that purpose; and (iii) where Special Category Data / Criminal Offence Data is processed, the conditions for processing such data are identified.

Code Member Criteria & requirements in detail		
7. Protection of children's interests	The Code Member pays particular attention to processing the Personal Data of children.	Evidence may include extracts from portfolios, LIAs or DPIAs or completing the ICO's self-assessment risk tool as found here for any pieces of work relating to children.
8. Criminal convictions register	Code Members must not maintain a comprehensive register of criminal convictions.	An annual written declaration confirming on-going compliance or alternative evidence which is accepted by the MB in its discretion.
9. Case Extracts – Legitimate Interests	The LIAs must determine the lawful basis for processing in accordance with Article 6(1)(f) of the UK GDPR. The three part test from the ICO's guidance here should be correctly applied.	A sample of up to three LIAs from live cases conducted by the Code Member which reflect the Code Member's range of services during the previous 12 months, as required by the MB. The MB will take into consideration that the business may not regularly carry out LIAs.
10. Lawful basis (legitimate interests – trace or locate)	The Code Member has considered and recorded the lawful basis appropriately in respect of Personal Data processing with reference to trace or locate instructions. Code Members are required to determine the appropriate lawful basis for processing and, where relying on legitimate interests as the lawful basis, keep a record of the LIA completed. In completing the LIA, the Code Member applies the three-part test.	There is no standard form for documenting the lawful bases for processing Personal Data, however Code Members must ensure that they can demonstrate that a lawful basis applies. This should explain, where relevant, any difference between the processing undertaken prior to locating an Individual and after locating an Individual. The Code provides guidance on this (see Part B paragraph 33 above) and the Code Member should use that guidance to support the evidence of the thought process in reaching a decision and justification of the outcome. Evidence may be required of any LIA undertaken, which includes the thought process in

Code Member Criteria & requirements in detail		
		reaching a decision and justification of the outcome. Code Members must include evidence confirming that: (i) the purposes of processing activities have been reviewed and the most appropriate lawful basis has been chosen; (ii) the processing is necessary for the relevant purpose, and they are satisfied that there is no other reasonable and less-intrusive way to achieve that purpose; and (iii) where Special Category Data / Criminal Offence Data is processed, the conditions for processing such data are identified.
11. Complaints	Code members must respond to Individuals' complaints received in accordance with the Code and guidance from the ICO. The MB may also investigate alleged breaches of the Code, and the Code Member must communicate with the MB in accordance with the Code and the cooperation criteria.	Evidence of any complaints received by the Code Member from Individuals in relation to data protection and the steps the Code Member took to respond to the complaint and where relevant, evidence that in relation to MB investigations of alleged breaches of the Code, the Code Member has communicated with the MB in accordance with the Code and the cooperation criteria in this Code ("Cooperates with the MB").

Code Member Criteria & requirements in detail		
12.Co-operates with the MB	Evidence that the Code Member has responded, or is able to respond, to any correspondence from the MB in full and address/remedy all issues raised within the required timeframe.	Code Members must provide a written response and enclose any relevant evidence to show that they are able to comply with the MB's requests which may include providing evidence of operational email accounts. Where the MB has communicated with the Code Member, the Code Member must provide evidence to show that it has corresponded appropriately with and cooperated with the MB, including in relation to any investigations of alleged non-compliance with the Code.
13. Address non-conformity report(s) (NCRs).	Full and adequate response to an NCR addressing and remedying all issues raised within the required timeframe.	Code Members must respond to an NCR issued by the MB by setting out in detail how they seek to address an NCR. Required actions may include updating DPIAs and LIAs to ensure compliance with Data Protection Law and providing further evidence of the lawful basis for processing Personal Data.
14. Knowledge	The Code Member has sufficient working knowledge of Data Protection Law.	Code Members are expected to be sufficiently knowledgeable in areas of Data Protection Law and procedure relating to Code Services, as covered in the Code. Applicants and Code Members may be asked specific questions on past work and should be able to demonstrate they are sufficiently knowledgeable about relevant Data Protection Law, as covered in the Code.