POLICY – DATA PROTECTON

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

- the data protection principles with which the Institute of Barrister's Clerks (the IBC) 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, e.g. 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 [insert name and/or position].

1 Introduction

1.1 The IBC 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 IBC Data Protection Privacy Notices.

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 [insert name and/or position]is responsible for data protection compliance within the IBC. If you have any questions or comments about the content of this policy or if you need further information, you should contact [insert name and/or position] on [insert email address and/or telephone number].

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 IBC's Data Protection Privacy Notice and, where appropriate, to its other relevant policies including in relation to internet, e-mail and communications [insert any other policies such as monitoring, social media, etc.], 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 before 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	(also 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	(also known as 'special categories of personal data', 'special category 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 IBC 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 is 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 is 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, i.e.:

(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 IBC is subject;
(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
(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 IBC 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 (i.e. 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 IBC'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' 'special category data' or 'sensitive personal data'.

6.2 The IBC 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, e.g. it is necessary for the performance of the employment contract, to comply with the IBC's legal obligations or for the purposes of the IBC's legitimate interests; and

6.2.2 one of the special conditions for processing sensitive personal information applies, e.g.:

(a) the data subject has given explicit consent;
(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the IBC 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 [insert name and/or position] of the proposed processing, in order that [insert name and/or position] 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 IBC will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

6.6 The IBC's Data Protection Privacy Notice sets out the types of sensitive personal information that the IBC processes, what it is used for and the lawful basis for the processing.

6.7 In relation to sensitive personal information, the IBC 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.

6.8 **During the recruitment process**: [insert name and/or position], with guidance from [insert name and/or position of person responsible for data protection], will ensure that (except where the law permits otherwise):

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

6.8.2 if sensitive personal information is received, e.g., the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

6.8.3 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;

6.8.4 '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;

6.8.5 we will [not ask health questions in connection with recruitment **OR** only ask health questions once an offer of employment has been made].

6.9 **During employment**: [insert name and/or position], with guidance from [insert name and/or position of person responsible for data protection], will process:

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

6.9.2 sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. [Where possible, this information will be anonymised]; and

6.9.3 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 Appendix 1 of this 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 (e.g. where the IBC 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 [insert name and/or position of person responsible for data protection] in order that a DPIA can be carried out.

8.3 During the course of any DPIA, the IBC will seek the advice of the [insert name and/or position of person responsible for data protection]and the views of [a representative group of] employees and any other relevant stakeholders.

9 Documentation and Records

9.1 We will keep written records of processing activities [which are high risk, i.e. 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 IBC's organisation [(and where applicable, of other controllers, the employer's representative and person responsible for data protection)];

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 relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;]

9.1.6 where possible, retention schedules; and

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

9.2

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

9.3.1 information required for privacy notices;

9.3.2 records of consent;

9.3.3 controller-processor contracts;

9.3.4 the location of personal information;

9.3.5 DPIAs; and

9.3.6 records of data breaches.

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

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

9.4.2 the lawful basis for our processing; and

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

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

9.5.1 carrying out information audits to find out what personal information the IBC holds;

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

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

9.6 [We document our processing activities in electronic form so we can add, remove and amend information easily.]

10 Privacy Notice

10.1 The IBC 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—see the IBC's Data Protection Privacy Notice;

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 IBC'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 [insert name and/or position of person responsible for data protection].

12 Individual Obligations

12.1 Individuals are responsible for helping the IBC keep their personal information up to date. You should let [insert name and/or position] know if the information you have provided to the IBC changes, for example if you move house or change details of the bank or building society account to which you are paid. [Alternatively, you can update your own personal information on a secure basis via the IBC's intranet.]

12.2 You may have access to the personal information of other members of staff, suppliers and customers/clients of the IBC in the course of your employment or engagement. If so, the IBC 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 IBC staff to access personal information if they have appropriate authorisation;

12.3.3 only allow individuals who are not IBC staff to access personal information if you have specific authority to do so from [insert name and/or position of person responsible for data protection];

12.3.4 keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions communicated to you by the IBC from time to time;

12.3.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the IBC'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 [insert name and/or position of person responsible for data protection]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 IBC'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 IBC will use appropriate technical and organisational measures [in accordance with the IBC's policies] 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 IBC 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 IBC;

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 IBC and under a written contract;

13.2.5 the organisation will assist the IBC in providing subject access and allowing individuals to exercise their rights in relation to data protection;

13.2.6 the organisation will assist the IBC in meeting its 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 IBC as requested at the end of the contract; and

13.2.8 the organisation will submit to audits and inspections, provide the with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the IBC 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 [insert name and/or position of person responsible for data protection].

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 [insert name and/or position of person responsible for data protection].

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 IBC 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 IBC will not transfer personal information outside the UK, or to international organisations.

OR

The IBC may transfer personal information outside the UK [to [insert name of country] and/or to international organisations on the basis [that that country, territory or organisation is designated as having an adequate level of protection

OR that the organisation receiving the information has provided adequate safeguards by way of [binding corporate rules **OR** standard data protection clauses **OR** of compliance with an approved code of conduct]].]

17 Training

The IBC 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 IBC 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 IBC; 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 [insert name and/or position of person responsible for data protection].

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

Signed: _____

Name: _____

Date: _____

APPENDIX 1 – CRIMINAL RECORDS INFORMATION

1.1 This Appendix 1 supplements the IBC's Data Protection Policy.

1.2 This document sets out the IBC's policy on asking questions about a prospective (or existing) employee's criminal record, and carrying out Disclosure and Barring Service (DBS) checks.

1.3 The IBC is committed to compliance with the DBS Code of Practice and our data protection obligations, to treat prospective employees fairly and not to discriminate unfairly against any subject of a criminal record check on the basis of a conviction or other information revealed. This Appendix 1 sets out how we comply with our data protection obligations in respect of criminal records information and seek to protect such information, and to ensure that staff understand and comply with the rules governing the collection, use and deletion of criminal records information to which they may have access in the course of their work.

1.4 We are committed to complying with our data protection obligations and the DBS Code of Practice in relation to criminal records information, in particular:

1.4.1 in relation to the circumstances in which we seek criminal records information;

1.4.2 by being concise, clear and transparent about how we obtain and use such information, and how (and when) we delete it once it is no longer required; and

1.4.3 by ensuring the correct handling, use, storage, retention and disposal of DBS certificates and certificate information.

2 Policy Statement - Criminal Records Information

2.1 Having a criminal record will not necessarily bar you from working with us. We will take into account the circumstances and background of any offences and whether they are relevant to the position in question, balancing the rights and interests of the individual, our employees, customers/clients, suppliers and the public.

2.2 We will treat all applicants, employees and volunteers fairly but reserve the right to withdraw an offer of employment if you do not disclose relevant information, or if a DBS check reveals information which we reasonably believe would make you unsuitable for the role.

3 Scope and Definitions

3.1 This Appendix 1 applies to criminal records information relating to job applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

3.2 Staff should refer to the IBC's Data Protection Policy and Data Protection Privacy Notice] and, where appropriate, to its other relevant policies.

3.3 We will review and update this Appendix 1 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 Appendix 1 to staff before it is adopted.

3.4 The definitions set out in the IBC's Data Protection Policy apply to terms used in this Appendix 1.

4 Asking for Criminal Records Information

4.1 Before recruiting for any post [insert name and/or position] will, with advice from [insert name and/or position of person responsible for data protection], assess whether it is justified in seeking criminal records information for that particular post (see paragraph 4.3 below) and, if so:

4.1.1 whether it is appropriate to limit the information sought to offences that have a direct bearing on suitability for the job in question; and

4.1.2 whether the information should be obtained from the individual or the DBS.

4.2 If an assessment under paragraph 4.1 has been carried out for the same or a similar post within the last [12] months, [insert name and/or position] may rely on that assessment.

4.3 The IBC will be justified in obtaining criminal records information for a particular post if it is necessary:

4.3.1 for the performance of the employment contract for that post;

4.3.2 in order for the IBC to comply with a legal obligation to which it is subject;

4.3.3 in order to protect the vital interests of [insert relevant description e.g., vulnerable service users]; and/or

4.3.4 for the purposes of the IBC's legitimate interests.

4.4 The level of criminal records information and DBS check that the IBC is entitled to request (i.e. a criminal records certificate (CRC) or enhanced criminal records certificate (ECRC)) will depend on the post for which the prospective employee's suitability is being assessed. Further details are set out in Appendix 2.

4.5 We will only ask for criminal records information once the employee has a conditional offer of employment.

4.6 We will only ask an individual to provide criminal records information in relation to convictions and cautions that the IBC would be legally entitled to see in a DBS check for the relevant post (see paragraph 4.4 above), i.e.:

4.6.1 if the IBC is justified in seeking criminal records information for the post, [and the post is not exempt from the Rehabilitation of Offenders Act 1974], we will ask the individual to complete the criminal records information form set out in [insert description of document], which states that individuals are not required to disclose convictions that are spent under the Rehabilitation of Offenders Act 1974; and

4.6.2 [if the IBC is justified in seeking criminal records information for the post, [and the post is exempt from the Rehabilitation of Offenders Act 1974], we will ask the individual to complete the criminal records information form set out in [insert description of document], which asks individuals if they have any convictions, cautions, reprimands or final warnings which are not filtered (or 'protected' as defined by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended)). For further information on filtering, see Appendix 2.]

4.7 If the information sought can be limited to offences that have a direct bearing on suitability for the job in question, the HR department will amend the criminal records information form accordingly.

4.8 Where a DBS check is identified as necessary, all application forms, job adverts and recruitment briefs will contain a statement that an application for a DBS certificate will be submitted in the event of the individual being offered the position.

4.9 Applicants will only be asked to complete a criminal records information form before an offer of employment is made unconditional; they will not be asked to do so during the earlier short-listing, interview or decision-making stages.

4.10 Before an individual is asked to complete a criminal records information form, they will be provided with a copy of this policy.

4.11 If the IBC is not justified in seeking criminal records information for the post, it will not ask an applicant for criminal records information.

4.12 If it is assessed that the IBC should use the DBS to verify criminal records information, the IBC will:

4.12.1 provide the individual concerned with a copy of the IBC's data handling policy (set out in Appendix 3) before asking them to complete a DBS application form or asking for their consent to use their information to access the DBS update service;

4.12.2 make every subject of a DBS check aware of the existence of the DBS Code of Practice and makes a copy available on request. A copy is available from www.gov.uk/government/publications/dbs-code-of-practice; and

4.12.3 comply with the DBS Code of Practice.

4.13 [The IBC will not rely on a previously-issued DBS certificate.]

4.14 Once criminal records information has been verified through a DBS check, the IBC will:

4.14.1 if inconsistencies emerge between the information provided by the individual and the information in the DBS certificate, give the applicant the opportunity to provide an explanation in accordance with paragraph 5;

4.14.2 record that a DBS check was completed and whether it yielded a satisfactory or unsatisfactory result; and

4.14.3 delete the DBS certificate and any record of the information contained in it unless, in exceptional circumstances, [insert name and/or position of person responsible for data protection] assesses that it is clearly relevant to the ongoing employment relationship [e.g. to allow for consideration and resolution of any disputes or complaints].

4.15 If, in accordance with paragraph 4.14.3, [insert name and/or position of person responsible for data protection] assesses that the information in the DBS certificate is relevant to the ongoing employment relationship, it (and any record of the information contained in it) will be kept securely for no longer than is necessary (usually no more than six months), and then destroyed.

4.16 The IBC will not seek criminal records information from any source other than the individual concerned or the DBS.

4.17 DBS certificate information will be handled and kept in accordance with the IBC's policy on handling DBS certificate information set out in Appendix 3.

5 Where an Unprotected Conviction or Caution is Disclosed

5.1 If the IBC has concerns about the information that has been disclosed by the DBS, or the information is not as expected, the IBC will discuss its concerns with the prospective employee and carry out a risk assessment.

5.2 [The IBC has a legal duty, when recruiting staff to work in regulated activity with children or vulnerable adults, to check whether they are on the relevant children's or adults' barred list. If a prospective employee's name does appear on the relevant barred list, it would be against the law for the IBC to employ them to work or volunteer with the relevant group.]

5.3 [If a prospective employee is not barred from working with the relevant group, but nevertheless has a criminal record, it is up to the IBC to decide on their suitability for the role. The IBC will not refuse a prospective employee employment simply on the basis that they have a criminal record. Before making a decision, the IBC will:

5.3.1 give the prospective employee the opportunity to address its concerns before making any decisions; and

5.3.2 carry out a risk assessment.]

5.4 In carrying out a risk assessment, the IBC will take account of:

5.4.1 the relevance of the conviction or other matter revealed to the position in question;

5.4.2 the seriousness of the offence or other matter revealed;

5.4.3 the circumstances of the offence;

5.4.4 the age of the offence;

5.4.5 whether there is a pattern of offending; and

5.4.6 whether circumstances have changed since the offending took place.

6 Training

6.1 The IBC will ensure that all those within the organisation who are involved in the recruitment process:

- have been suitably trained to identify and assess the relevance and circumstances of offences; and
- have received appropriate guidance and training in the relevant legislation relating to the employment of ex-offenders, e.g., the Rehabilitation of Offenders Act 1974.

APPENDIX 2 – LEVEL OF DBS CHECK AND FILTERING

1. Requesting a DBS Certificate

The level of DBS check that the IBC is entitled to request will depend on the position for which the prospective employee's suitability is being assessed. The IBC may request:

- A Criminal Record Certificate (CRC) if the position is excepted form the protections of the Rehabilitation of Offenders Act 1974 (i.e. included in the Rehabilitation of Offenders (Exceptions) Order 1975, as amended);

- A Enhanced Criminal Record Certificate (ECRC) if the position is (a) excepted from the protections of the Rehabilitation of Offenders Act 1974 (i.e. included in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, as amended; and (b) prescribed in the Police Act 1997 (Criminal Records) Regulations 2002 [and, in addition, a search of the [children's **OR** adults'] barred list if the position is eligible for an ECRC and prescribed in the Police Act 1997 (Criminal Records) Regulations 2009 as one for which the [children's **OR** adults'] barred list may be checked].

2. Filtering of Protected Convictions and Cautions

Certain old and minor convictions and cautions are 'protected' which means:

- They are filtered out of a DBS check;

- They need not be disclosed by prospective employees to the IBC; and

- They will not be taken into account by the IBV in making decisions about employing a prospective employee.

Certain 'listed offences' will never be filtered out (see: www.gov.uk/government/publications/dbs-list-of-offences-that-will-never-be-filtered-from-a-criminal-record-check). The list includes offences which are particularly serious, relate to sexual or violent offending or are relevant in the context of safeguarding.

A conviction will be a protected conviction (i.e. filtered) if:

- The offence was not a listed offence;

- It did not result in a custodial sentence (or sentence of service detention);

- It is the individual's only conviction; and

- Where the individual was an adult at the time of convictions, 11 or more years have passed since the date of the conviction (or five years six months or more have passed since the date of conviction if the individual was under 18 at the time of conviction).

A caution will be a protection caution (i.e. filtered) if:

- The offence was not a listed offence; and

- Where the individual was an adult at the time of the caution, six year or more have passed since the date of the caution (or two years or more have passed since the date of conviction if the individual was under 18 at the time of conviction).

As part of an ECRC, the police may also disclose information that they reasonably believe is relevant and ought to be included.

Further guidance on filtering is available at:
www.gov.uk/government/collections/dbs-filtering-guidance

APPENDIX 3 – DATA HANDLING

1. Storage and Access

The IBC will ensure that DBS certificate information is kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

2. Handling

In accordance with section 124 of the Police Act 1997, the IBC will ensure that certificate information is only passed to those who are authorised to receive it in the course of their duties. The IBC maintains a record of all those to whom certificates or certificate information has been revealed. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

Once the DBS certificate has been inspected, it will be destroyed in accordance with the code of practice.

3. Usage

Certificate information must only be used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

4. Retention

Once a recruitment (or other relevant decision) has been made, the IBC does not keep certificate information for any longer than is necessary. This is generally for a period of up to six months, to allow for consideration and resolution of any disputes or complaints.

If, in very exceptional circumstances, it is considered necessary to keep certificate information for longer than six months, we will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so.

Throughout this time, the usual conditions regarding safe storage and strictly controlled access will prevail.

5. Disposal

Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means e.g. by shredding, pulping or burning. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack).

We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.

6. DBS Logo

The IBC will not copy or use the DBS logo without prior approval of the DBS.

[7. Acting as an Umbrella Body

Before acting as an umbrella body (an umbrella body being a registered body which countersigns applications and receives certificate information on behalf of other employers or recruiting organisations) we will take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and dispose of certificate information in full compliance with the code of practice and in full accordance with the appendices to this Data Protection Policy.

We will also ensure that any body or individual, at whose request applications for DBS certificates are countersigned, has such a written policy and, if necessary, will provide a model policy for the body or individual to use or adapt for this purpose.]