Policy and procedures for the storage, use and disposal of sensitive or confidential information

(including Disclosure and Barring service application related materials) [1]

1 Introduction and General Principles

1.1 The Interdenominational Protection Panel (IPP) was established in 2001 to support, advise and assist the Union of Welsh Independents, Baptist Union of Wales and the Presbyterian Church of Wales in relation to safeguarding practice in their work with children and young people and vulnerable adults. The Panel is a registered body responsible for processing Disclosure and Barring service (DBS) checks for employees and volunteers within the three denominations and helps assess the suitability of applicants for positions of trust within these denominations.

1.2 In 2008 the Panel became an Umbrella Body enabling it to process disclosure checks for organisations and agencies who are not members of the above three denominations.

1.3 The Interdenominational Protection Panel complies with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

1.4 The Interdenominational Protection Panel complies with their obligations under the Data Protection Act and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of Disclosure information and other confidential, sensitive or financial information in the execution of its business.

2 Storage and Access

2.1 The Interdenominational Protection Panel does not hold personnel files for DBS applicants. The procedures outlined in the Safeguarding Vulnerable Groups handbook advises churches, as part of their safer recruitment and selection process, to ask volunteers to complete an application and Self-declaration form. These forms are for local church decision making and should be stored locally in a secure and confidential manner.

2.2 Any information held by the Panel in relation to DBS applications is kept securely, in lockable, non-portable, storage containers. Access is controlled and limited to the Lead Counter Signatory, the Safeguarding Officer and the Administrative Officer of The Interdenominational Protection Panel, and those who are entitled to see it as part of their duties according to the agreed policy of The Panel in relation to the handling of blemished disclosures

2.3 Any information shared with the Panel in relation to safeguarding concerns of any nature is kept securely, in lockable, non-portable, storage containers. Access is controlled and limited to those who need to see it as part of their duties. Such information would be shared with statutory agencies where there were concerns about the safety of a child or vulnerable adult.

2.4 In accordance with section 124 of the Police Act 1997, Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Disclosures or Disclosure information has been revealed and we recognise that it is a Criminal Offence to pass this information to anyone who is not entitled to receive it.

2.5 **Usage:** Disclosure information is only used for the specific purpose for which it was requested. Since June 2013 a single DBS certificate is issued by the DBS and sent directly to the applicant. It is the responsibility of the applicant to forward this certificate to the Interdenominational Protection Panel Office to complete the application process.

[1] 1This policy is in addition to the Policy statement on the secure handling, use, retention and disposal of disclosures and disclosure information. (Safeguarding Vulnerable Groups Handbook – Appendix 5)

2.6 **Retention**: Once a recruitment (or other relevant) decision has been made, the disclosure certificate is returned to the applicant and any related information is securely disposed of. This process should not exceed a period of up to six months, to allow for the consideration of any information contained within the disclosure and resolution of any disputes or complaints.

We will not keep a photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure with the exception as noted in 2.6 and 3.3.2. If, in exceptional circumstances, it is considered necessary to keep the disclosure 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 individual subject before doing so. Throughout this time, the usual conditions regarding safe storage and strictly controlled access will prevail.

2.7 Notwithstanding the above, we may keep a record of the date of issue of a Disclosure, the name of the subject and their address at the time of the application, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number and the details of the recruitment decision taken. This will assist with the processing of future repeat DBS applications and dealing with any queries or concerns. If a Contract is drawn up as a result of the disclosure any information necessary to enable the effective review of the contract may be retained and securely stored.

2.8 Identifiable information relating to the disclosure will be destroyed when a decision regarding the appointment has been made with the exceptions as noted above.

2.9 **Acting as an Umbrella Body**. As an Umbrella Body (one which countersigns applications and receives Disclosure information on behalf of other employers or recruiting organisations), we will take all reasonable steps to ensure that organisations using this service can comply fully with the DBS Code of Practice. We will also take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and dispose of Disclosure information in full compliance with the DBS Code and in full accordance with this policy. We will also ensure that any organisation or individual, at whose request applications for Disclosure are countersigned, has such a written policy and, if necessary, will provide a model policy for that body or individual to use or adapt for this purpose.

3 Disposal of confidential documentation

3.1 We will ensure that any sensitive or confidential material is destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, Disclosure information will not be kept in any insecure receptacle.

Identifiable information relating to disclosures will be destroyed by secure means when a decision regarding the appointment has been made with the exceptions as noted at 2.6 and 4.1.3.

Appendix 1
Procedures relating to specific documentation or situations

1 DBS certificates and related information

1.1 "Clear disclosure certificates" (one showing no information relating to convictions, police information etc.)

The Interdenominational Protection Panel will note the date and number of the certificate, the name and address of the applicant, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number and the details of the recruitment decision taken. This will assist with initiating future DBS renewal applications and in dealing with any queries or concerns.

The original certificate will be returned to the applicant within 10 working days. No copy of the certificate will be made.

The secretary of the relevant church or body will be informed that the DBS process has been completed and that the applicant is able to start or continue with their role. (See also 2.6 above).

1.2 "Blemished disclosure Certificates" (one showing convictions, cautions, reprimands, final warnings or information from the police)

- The Panel Office will contact the applicant to ask for confirmation that the information is correct and to ask for any further details or mitigating circumstances. Occasionally the Panel may need to seek further information from third parties regarding the individual or the conviction in order to make an informed decision. All information will be stored and disposed of following the principles and procedures as noted above.
- A risk assessment will be carried out and a Confidential Panel will be convened to discuss the case. Information shared with the Panel members in order to make a decision will usually be anonymised unless this seriously impairs the decision making process.

Informing relevant parties of a decision:

- The applicant and the employer will be informed of the decision in writing. In some circumstances it may be appropriate to arrange a meeting to share information effectively and sensitively. Professional Advice may be sought on the amount or the most appropriate way to share confidential information with the interested parties and trustees.
- If appropriate a referral will also be made to the DBS or to statutory authorities or advice sought.
- If it is unlawful for the person to work with children and /or vulnerable adults the Panel will write to the individual, the denominational General Secretary and the responsible parties within the local church (this will usually be the minister and trustees) to inform them of this.
- Frequently the Panel advises that there is *no specific risk* related to the disclosure and the individual is able to proceed with the work. In some cases this Panel may advise that the individual can work or volunteer but may *make recommendations or suggest conditions* or offer advice to further safeguard an individual applicant or other parties. Information regarding such recommendations or advice will be shared on a need to know basis.
- If the Panel, following consideration of the information and circumstances, believes that it would be inappropriate or inadvisable (rather than illegal) for the individual to proceed with the role the panel will offer advice and recommendations to the employing church or organisation. Information related to such recommendations or advice will be shared on a need to know basis. Confidentiality would be stressed in such circumstances.
- At the end of the decision making process the original certificate will be returned to the applicant.

Storage of related information: If a Contract is drawn up as a result of the information contained in the disclosure or if the case will require review in the future, any relevant information may be stored securely to enable the review to happen effectively.

1.3 Additional Future Disclosures

The Panel office will keep a securely stored confidential log of previous blemished disclosures and decisions made. This will enable further additional future disclosures to be dealt with quickly and effectively.

A further disclosure containing the same information as the earlier disclosure will be reviewed by the Safeguarding Officer and a Countersignatory and, unless further concerns are raised, the previous decision will be upheld. If the disclosure contains new or additional information the blemished disclosure process will recommence.

2 Self- declaration Forms sent to the Panel Office

2.1 An applicant has the option to send self-declaration form to the panel office if they do not wish to disclose details of sensitive issues locally. These will be dealt with as per blemished DBS disclosure certificates and information will be shared with the local church and General Secretary as per the confidential panel decision (See 1.2 above)

2.2 Any applications forms or self-declaration forms sent to the Panel Office in error will be dealt with securely. The applicant will be contacted and it will be agreed how to proceed. E.g. – return to the applicant or to the church secretary.

3 Information relating to known abusers, cases of abuse or suspected abuse

3.1 Concerns or suspected abuse: Any information shared with the Panel concerning possible abuse or other confidential concerns will be dealt with confidentially and stored in non-portable lockable containers. Such information would be shared with statutory authorities, general secretaries of the relevant denomination and local trustees or responsible individuals as appropriate. Where there is a reason to retain such information (to enable future review) this will be stored securely in a lockable and non-portable container.

3.2 **Contract with a known abuser:** If information concerning a crime or known abuse is to be used to develop a contract between a known abuser and a local church this will be stored securely and shared confidentially with appropriate statutory authorities and named responsible local church leaders or trustees. Any relevant information will be stored securely in order to assist with the review of such contracts in the future. The local church is responsible for storing any shared information securely. The church will be responsible for the review process with the Panel officials available to offer advice. Any information will be disposed of securely when there is no further reason to retain it.

3.3 **Any information pertaining to suspected or historical abuse** will be shared with the appropriate statutory authorities and disposed of securely when there is no further reason to retain it.

4 Accounting and financial documentation

4.1 Accounting information and other information held in relation to the Panels operation as a company limited by guarantee will be kept for 6 years plus the current financial year in line with guidelines as is required as a Company limited by guarantee. At the end of this period they will be disposed of. Financial Documents will be shared with the Panel accountant and Panel members as appropriate