**Protocol for Parishes who will be using the DBS e-bulk System**

**Introduction**

In order for the parish/benefice to sign up to the use of the Disclosure and Barring Service (DBS) e-bulk system, the DBS and the Diocese of Bath and Wells need to be assured that standards of both physical and electronic data security and confidentiality will be maintained. Training will be provided so that you can understand your role within this process, and know who to contact should you have any queries.

**Registration and de-registration process**

Attached to this protocol is a form which anyone accessing the DBS computer systems will be required to sign. This confirms that you have read and understood this protocol, and that you agree to keep to the standards within it as a condition of being given access to the DBS electronic system via our providers, Security Watchdog (part of the Capita Group). Once we have received this signed form from you, a log-in and password will be created to allow you to access the system. You must keep these log-in details secure and not share them with any other person, or allow anyone else to access the system using your log-in details. Any person accessing the DBS electronic systems must have their own log-in so that a clear audit trail can be kept.

If at any point you leave your role in the parish, or no longer need to have access to the system for any other reason, you agree to advise us so that your log-in can be removed from the system. A new form will need to be completed for a replacement log-in to be created for any new or additional person in the parish needing to access the system.

**Data Protection**

Under the Data Protection Act you are obliged to inform any person whose information you will be accessing through the electronic DBS system

* That you will be entering data provided to you into an electronic storage system
* That the data will be processed and used only for the purposes of obtaining a DBS check
* That you may receive the results of that check electronically, and you may record it manually or electronically
* That you will retain the data only for as long as you need to in order to meet the requirements of the purpose for which you have obtained it. Further information about keeping data can be found in the Diocesan Data Retention Policy.
* That the data will be kept securely at all times, and destroyed when no longer needed.

**Confidentiality**

Information provided to you by people having a DBS check, and information you receive as a result of that check is to be treated as confidential. You must take every possible step to ensure that the data remains private and never knowingly release any confidential information to anyone else without the consent of the person the information belongs to. You must therefore advise anyone providing you with information for a DBS check that the outcome of their check, that is, being clear or containing information about cautions convictions or other police intelligence may be recorded on your manual or electronic system, and will also be shared with the Diocesan Safeguarding Team, and potentially with other Church Officers if relevant to the role for which they have applied or are undertaking. If they do not consent to this, you may not be able to continue with the DBS checking process and should seek advice from the Diocesan Safeguarding Adviser.

**Physical security of data**

In order to ensure that confidential data is kept secure, any paper copies of personal information, documents, or printouts of DBS check results, from whatever source, should be stored in a secure place. This could be a locked filing cabinet in the parish office, to which there is limited access; a secure file in the Incumbent’s office; or a locked file box/drawer in the Parish Safeguarding Officer’s home; or similar secure arrangements. Wherever the data is kept it should always be locked away when not in use, and only be accessible to those who are authorised to access it. Any information no longer required should be returned to the data owner (the person it is about) or securely shredded so that it cannot be read by any unauthorised person. When the office where the data is stored is not in use, the doors and windows should be locked to ensure that unauthorised persons cannot gain access to the data.

**Computer and IT System Security**

You will be given access to the DBS computer network to assist you in performing your role for the parish. It is important that in order to maintain the integrity of the security in the system you use the computer accessing the DBS network responsibly, professionally, ethically and lawfully. The integrity of computer and network systems must be protected by appropriate use of firewalls, anti-virus software and regular system updates to address any vulnerabilities in software. Users should consider whether any of the sites visited by any users of the computer could be prone to virus infection (for example, sites containing inappropriate or sexually explicit material) and limit access to those sites using parental controls or other blocking software.

Computer access should be protected by the use of a personal log-in and password, and where the computer is used by more than one person a log-in and password for each user, and confidential data should not be sharable between users. If necessary to secure the data, individual electronic documents containing confidential and DBS information should be password protected. If the computer is not in use, it should be switched off; the computer should automatically default to needing a password to log back in if it is left on and unused for a short period of time not exceeding 5 minutes.

Electronic data that is no longer required must be securely deleted to ensure that it is not inadvertently made available. This means deleting it off the system, and ensuring it is also deleted from any other electronic storage media such as email, external hard drives and memory sticks. It should then also be deleted from the “Recycle Bin” on the computer so that it cannot be accessed by other users. If the computer is to be disposed of at a later date, it may be necessary to have the hard drive professionally wiped or physically destroyed to ensure that there is no loss of confidential data.

**Limitations on Use**

Access to the DBS e-bulk system, via the Security Watchdog network is provided only for the purpose of carrying out DBS checks on people whose role within the parish requires them to have such a check. It must not be used for any other purpose, including carrying out checks on people who do not have a role within the parish, or who do have a parish role, but where that role does not require them to have a DBS check.

**Request to Sign up to use the DBS e-bulk facility**

**I have read the attached Protocol and understand my responsibilities in ensuring that my use of the DBS e-bulk system is ethical, secure and lawful. I agree to follow the *Protocol for Parishes who will be using the DBS e-bulk System* at any time I am undertaking a DBS check, or using a computer or other digital device on which I connect to the DBS /Security Watchdog systems, or on which I store any confidential or DBS related information. I will advise the Diocesan Safeguarding Team if my tenure in this role comes to an end and I no longer need to be registered to access the system.**

Name of applicant: …………………………………………………………………………………………………………………

Role of Applicant: ……………………………………………………………………………………………………………………

Name of Parish/Benefice for which checks will be carried out: …………………………………………………

………………………………………………………………………………………………………………………………………………….

Deanery parish/benefice is in: ………………………………………………………………………………………………….

Signature of Applicant: ……………………………………………………………………………………………………………….

Date: …………………………………………………………………………………………………………………………………………..

Authorisation of applicant for this role by (incumbent/PCC Chair): ………………………………………………

**In authorising the above applicant to carry out this role I confirm that I have read the *Protocol for Parishes who will be using the DBS e-bulk System*, and confirm that this process will be adhered to in the parish/benefice above.**

Name of Authoriser: ………………………………………………………………………………………………………………………..

Signature of Authoriser: ……………………………………………………………………………………………………………………

Date: …………………………………………………………………………………………………………………………………………………

Please return to the Diocesan Safeguarding Adviser, Diocese of Bath and Wells, The Old Deanery, Wells, BA5 2UG.

In case of any queries about the DBS or about this protocol, please contact the Assistant Diocesan Safeguarding Adviser on 01749 685103.