Handling of DBS Information Policy

Purpose

This policy sets out how the church body will collect, receive, handle, store, use, retain and dispose of Disclosure and Barring Service (DBS) certificate information and related records. Its purpose is to ensure that DBS information is managed lawfully, fairly, securely and only for legitimate safeguarding, recruitment, appointment and ministry purposes, in line with the [Church of England]() Safer Recruitment and People Management Code of Practice, the [Church of England]() guidance on DBS checks, the Police Act 1997, the UK General Data Protection Regulation and the Data Protection Act 2018.

Scope

This policy applies to the parish, benefice, parochial church council (PCC), and any other relevant Church of England church body using DBS information in connection with clergy, employees, volunteers, church officers and other appointed roles. It applies to incumbents, churchwardens, parish safeguarding officers, parish DBS administrators, PCC members where relevant, ministry leaders, volunteers and anyone else who receives, views, processes, stores or makes decisions using DBS information on behalf of the church body. It applies to information obtained through basic, standard and enhanced DBS checks, including barred list information where applicable, and to both paper and electronic records connected with safer recruitment, safeguarding, appointment, ministry and ongoing suitability assessments. [Church of England]() guidance makes clear that safer recruitment and people management applies to clergy, employees, volunteers and elected members within scope.

Definitions

For the purposes of this policy, DBS information means certificate information, disclosure content, certificate numbers, check type, date of issue, recruitment decisions linked to the check, and any notes or records created from reviewing the certificate. It does not include general recruitment records that do not reveal certificate content.

Roles and Responsibilities

The incumbent, priest-in-charge or other relevant church leader, together with the PCC and any delegated safeguarding or recruitment leads, are responsible for ensuring that this policy is implemented and reviewed. The parish safeguarding officer, parish DBS

administrator and anyone involved in safer recruitment or safeguarding must ensure DBS information is requested only where appropriate and lawful for the role, used only for legitimate decision-making, and shared strictly on a need-to-know basis. Clergy, lay leaders, staff and volunteers who handle DBS information must maintain confidentiality, follow secure storage requirements and report any actual or suspected breach immediately. Where diocesan safeguarding staff, diocesan safeguarding advisers or diocesan processes are involved, the church body must cooperate with them and follow diocesan requirements and advice.

Principles for Handling DBS Information

The church body will handle DBS information in accordance with the principles of confidentiality, necessity, proportionality and data minimisation. DBS information will only be obtained where a check is lawful and appropriate for the role and its activities, and the level of check must reflect the eligibility of the post under DBS law and [Church of England]() guidance. DBS information will only be used for the purpose for which it was requested, and only by authorised individuals in the course of their duties. The church body recognises that safer recruitment and people management is wider than DBS checking alone and must sit alongside proper role design, references, oversight, safeguarding culture and continued vigilance.

Storage and Access

Paper copies of DBS certificate information, where exceptionally held, must be kept in secure, lockable, non-portable storage with access limited to authorised personnel. Electronic records must be held within secure systems with appropriate access controls, passwords and, where available, encryption. DBS certificate information must not be stored on personal devices or in unsecured shared locations. Certificate information must not be kept on an individual's general personnel file unless there is a lawful and documented reason for retaining limited related information.

Use and Disclosure

DBS information will only be used for the specific purpose for which it was requested, such as assessing suitability for a church role, ministry, office, safeguarding decision-making or meeting a legal or regulatory requirement. Information from a DBS certificate will only be disclosed to those authorised to receive it in the course of their duties, which may include relevant parish officers or diocesan safeguarding personnel where this is necessary and lawful. A record should be maintained of any disclosure of certificate information. Unauthorised disclosure may constitute a criminal offence and may also result in disciplinary, capability, volunteer management or ecclesiastical action as appropriate.

Approved at PCC on 10th June 2026

Retention

Once a recruitment, appointment, licensing, authorisation or other relevant decision has been made, the church body will not retain DBS certificate information for longer than is necessary. In most cases, certificate information should be retained for no more than six months after the decision, unless there is a clear lawful basis for longer retention, such as an ongoing dispute, complaint, legal requirement, inspection, safeguarding audit need or formal church process. If information is retained beyond six months, the reason must be documented and the information must remain subject to the same security controls.

Disposal

When the retention period has expired, DBS certificate information must be destroyed securely and without delay. Paper records must be shredded or otherwise confidentially destroyed. Electronic records must be permanently deleted from relevant systems and locations in accordance with the organisation's records management procedures. The organisation will not keep photocopies, scans or other images of certificates, or any copy or representation of the certificate contents, unless there is a lawful basis and explicit justification for doing so.

Data Subject Rights and Privacy

Individuals whose information is processed under this policy have rights under applicable data protection legislation, subject to any legal exemptions. The organisation will process DBS information transparently, provide appropriate privacy information, and respond to rights requests in accordance with its data protection procedures. Where a decision may be affected by certificate content, the individual should be given an opportunity for appropriate discussion in line with fair recruitment practice.

Breach Reporting

Any actual, suspected or attempted loss, misuse, inappropriate access, unauthorised disclosure or security incident involving DBS information must be reported immediately through the organisation's data breach or incident reporting process. Incidents will be assessed promptly, contained where possible, investigated appropriately and escalated in line with legal, regulatory and organisational requirements.

Monitoring and Review

This policy will be reviewed periodically and updated where required to reflect changes in legislation, DBS guidance, diocesan requirements, safeguarding practice, Church of England policy and information security requirements. Compliance with this policy may

be monitored through parish or diocesan audits, safer recruitment checks, safeguarding reviews and incident management processes. Church bodies should ensure that those with responsibility for safer recruitment, safeguarding and DBS administration are appropriately trained and supported.