Chapter 3 – Information Sharing and Data Protection

Contents

1. Introduction

Context

1.1. The Catholic Church in England and Wales is committed to promoting a culture of safeguarding. To deliver on this goal, and to ensure best practice in safeguarding matters, a 'one church approach' that demonstrates responsible and effective information sharing is necessary.

1.2. Sharing information enables organisations to cooperate thus helping to ensure the young, those at risk and the vulnerable are given the protection they need. We are also mindful that sharing information presents risks if done insensitively and/or unlawfully. In addition to the legal risks, one risk of insensitively sharing information is that if those who disclosed the information find that it is shared in ways they did not expect, they may be less inclined to disclose such information in future.

1.3. The Catholic Church's national safeguarding structure (National Safeguarding Structure) comprises organisations and groups between which information, when appropriate, is shared. Partner organisations include: Dioceses, Religious Congregations, Catholic Voluntary Groups/Organisations, the Congregation of Religious, the Catholic Safeguarding Advisory Service and the National Catholic Safeguarding Commission.

1.4. The various organisations are in and of themselves separate legal entities. Information cannot be freely shared between organisations unless there is a clear and legitimate reason to do so.

1.5. This Chapter is intended to provide guidance to help all involved in safeguarding within the Catholic Church in England and Wales to make good decisions in relation to information sharing. It sets out the legal issues you must consider before sharing information, the governance arrangements which you must put in place, and provides a practical guide to making decisions about sharing information, including examples.

What is 'information sharing'?

1.6. There are two main types of information sharing. The first involves information that is shared within an organisation. The second is information that is shared with another organisation. This Chapter is primarily aimed at information that is shared between organisations and groups within the National Safeguarding Structure. However, the principles in this Chapter also apply to sharing information with organisations outside the National Safeguarding Structure, such as statutory agencies.

Who are you likely to share information with?

1.7. For safeguarding children and adults, where appropriate information may be shared with the following people, all of whom are required to keep information confidential within the boundaries of inter-agency professional confidentiality:

- The Safeguarding Representative
- The Safeguarding Coordinator
- The Safeguarding Lead in a Religious Congregation
- A member of the Safeguarding Commission
- The Bishop, Congregation Leader or their delegate
- The Catholic Safeguarding Advisory Service staff
- Members of the National Catholic Safeguarding Commission
- Children's Social Care Services professional staff
- Adult Social Care Services professional staff

- The Police
- The Probation Service(s)
- The National Society for the Prevention of Cruelty to Children

1.8. Information may also legitimately be shared with the Diocesan or Congregational Insurers where appropriate, with the Charity Commission to comply with the Serious Incident Reporting requirements and with legal advisors to obtain legal advice or handle legal proceedings. However, this is not an exhaustive list.

1.9. Any queries about information sharing must be directed to the relevant Data Protection Officer. It is recommended that the Safeguarding Coordinator and Data Protection Officer agree processes for dealing with data requests, for example, which decisions can be made by the Safeguarding Coordinator and which must be referred to the Data Protection Officer (e.g. disclosure of data outside the EEA).

1.10. The Safeguarding Co-ordinator must record in the relevant case file full details of all decisions regarding information sharing, including the rationale. It is recommended that the template information sharing protocol is used to record such decisions.

2. Legal issues

2.1. Information can only be shared between organisations in compliance with the law. The main considerations will be the law of confidence and data protection law. There are also specific rules around information obtained from the Disclosure and Barring Service.

Confidentiality

2.2. The law of confidence applies where information that is not widely known is given by one person to another in circumstances where both parties understand that the information is not to be passed on to anyone else.

2.3. When speaking to a child or an adult in circumstances where there are concerns about significant harm to a child or an adult, **full confidentiality cannot be promised**. Although an obligation of confidentiality can limit the circumstances in which information may be shared, it is possible to override the duty of confidentiality. For instance, it may become necessary to share the information in order to protect others as well as the person subject to the concerns. Information may need to be shared for a Child Protection Enquiry by Children's Social Care Services, and/or for a criminal investigation by the Police or for an adult investigation by Adult Social Care Services and/or in some circumstances it may be needed for action in the Courts or other legal proceedings or for insurance reasons.

2.4. It is important that it is explained to children, families and other adults, openly and honestly, what and how information will, or could be shared and why, and seek their understanding and, if necessary or appropriate, their consent.

2.5. Confidentiality is often confused with secrecy and remaining anonymous in reporting and referring. Anonymity can be agreed where the report is coming from a parishioner or member of the public and is being passed to the public agencies through the Safeguarding Representative, Religious Safeguarding Lead or the Safeguarding Coordinator, but only with their agreement and in agreement with the public agency e.g. the Police or Children's Social Care Services / Adult Social Care Services. Total anonymity cannot be guaranteed as the circumstances may develop into a criminal process.

2.6. If there are concerns about the safety of the person reporting, this must be clearly recorded and taken into full account when reaching an agreement with the Social Care Services and the Police.

2.7. Where a person in a formal role within the Church raises a concern or reports an allegation, they cannot do so anonymously.

Data protection law

2.8. The General Data Protection Regulation and the Data Protection Act 2018 set out the legal framework for how '**personal data**' must be managed. Personal data is defined as information relating to a living individual who is identified or identifiable. Data protection laws do not therefore apply to anonymised information where it is no longer possible to identify individuals. It is always worth considering whether information can be shared in an anonymous format, as this avoids the need to consider data protection issues.

2.9. Data protection laws regulate but do not prohibit the sharing of personal information. Instead, they set out a framework to ensure that such information is only shared where it is appropriate and lawful to do so.

2.10. Under data protection laws, the organisation responsible for the personal information (known as the **'controller'**) must always comply with the data protection principles and must always have a lawful basis for processing personal data. 'Processing' is defined widely and includes the sharing of personal data with another organisation.

2.11. Accordingly, whenever one organisation is considering sharing personal data with another organisation for safeguarding purposes, it must comply with the data protection principles and have a lawful basis for the sharing.

2.12. The data protection principles, set out in Article 5 of the GDPR, state that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to those purposes;
- accurate and, where necessary, kept up to date;
- not kept in a form that permits identification of individuals for longer than necessary;
- kept secure using appropriate technical and organisational measures.

<u>The lawful conditions for processing</u>

2.13. Data protection law requires that controllers must have a lawful condition for processing personal data. The lawful conditions are set out in Article 6 of the GDPR. At least one of the following must be met whenever personal data is processed:

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose;
(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract;
(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations);
(d) **Vital interests:** the processing is necessary to protect someone's life;
(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law;

(f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

2.14. For safeguarding issues, the most likely conditions to rely on will be legal obligation, legitimate interests and consent. Where there is an immediate concern for the health and safety of a specific individual, it may also be possible to reply on the vital interests condition.

2.15. If the personal data being shared includes one or more of the special categories of personal data, an additional condition is required. Information falls into a special category of personal data where it reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, sex life or sexual orientation, or the processing of genetic or biometric data for the purposes of uniquely identifying an individual.

2.16. The additional conditions for processing special categories of personal data are set out in Article 9 of the GDPR (and supplemented in Schedule 1 of the Data Protection Act 2018). The most likely conditions for sharing special categories of personal data for safeguarding purposes are:

- the data subject has given their explicit consent to the processing;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- processing is necessary for reasons of substantial public interest in certain defined circumstances (see part 2 of Schedule 1 of the Data Protection Act 2018).

2.17. In some cases, you must also have an 'appropriate policy document' in place to rely on these conditions. See Part 4 of this Chapter for more information about this requirement.

2.18. The GDPR prohibits the processing of personal data relating to criminal convictions and offences unless Member State or EU law permits its processing (subject to appropriate safeguards being in place). In the UK, organisations need to review the Data Protection Act 2018 to determine if there is a lawful condition set out within that legislation that will permit the necessary processing.

2.19. Schedule 1 Part 2 of the Data Protection Act 2018 contains specific 'substantial public interest' conditions that permit the processing of this type of information (these conditions are the same as for processing of special category information) with additional conditions applying only to the processing of criminal convictions and offences data set out in Schedule 1 Part 3.

2.20. The conditions under Schedule 1 that are likely to be most relevant for handling information for safeguarding purposes include:

- Paragraph 6 – statutory and government purposes
- Paragraph 7 – administration of justice and parliamentary purposes
- Paragraph 10 – preventing or detecting unlawful acts
- Paragraph 11 – protecting the public against dishonesty etc
- Paragraph 12 – regulatory requirements relating to unlawful acts and dishonesty etc
- Paragraph 17 – counselling
- Paragraph 18 – safeguarding of children and individuals at risk
- Paragraph 29 – consent
- Paragraph 30 – protecting individual's vital interests
- Paragraph 31 – processing by not-for-profit bodies

- Paragraph 33 – legal claims

2.21. It is recommended that you consult the relevant Data Protection Officer and/or the detailed guidance published by the Information Commissioner's Office (**ICO**) to determine which of these conditions you may be able to rely on before sharing any personal data. The ICO is the UK's statutory regulator for data protection law. The guidance can be found at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Individual rights requests

2.22. Under data protection law, individuals have a right to request copies of their own personal data. All such right of access requests should be referred to the diocesan or congregational Data Protection Officer. They will advise on the relevant procedures to follow.

2.23. The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

2.24. An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). For this reason, it is important to establish whether the information requested falls within the definition of personal data.

2.25. For further information about the definition of personal data please see the ICO guidance on what is personal data.

2.26. In addition to a copy of their personal data, individuals are also entitled to be provided with the following:

- the purposes of your processing;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

2.27. Much of this information might already be contained in diocesan or congregational privacy notices. For detailed guidance on processing right of access requests, see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Disclosure of Catholic Church 'Child and Adult Protection Records' in Court Proceedings

2.28. Requests for the disclosure of Catholic Church Child and Adult Protection records, i.e. case files and related material, may come from parties involved in either civil or criminal proceedings and may be made before any proceedings have started. Any party making such a request by telephone must be asked for written confirmation.

2.29. No voluntary disclosure should be given to anyone other than the individual (i.e. the data subject) and then only those personal records that he/she is entitled to under data protection law. Before disclosure is given, the Safeguarding Coordinator should liaise with the Data Protection Officer and, where necessary, legal advice should be sought as to the principles of disclosure and the extent of the same. Any legal advice should be obtained either through the Diocesan or Congregational Insurance Officer or for dioceses/congregations supported by the Catholic Insurance Service Ltd (**CIS**), by contacting the in house solicitor at CIS.

2.30. In **Civil cases**, any claim for damages, or intimation of such a claim, should have been reported to the relevant insurers (Management of Allegations and Concerns – national policy and procedure). The Insurers will have appointed solicitors who will manage any disclosure issue which arises in the course of such civil actions.

2.31. Where the Diocese or Religious Congregation receives a disclosure request where a civil claim has been intimated or is ongoing, the receiving Safeguarding Coordinator should not respond, but should pass the request forthwith to the insurance intermediary or direct to the appointed solicitors, who will consider it in the first instance.

2.32. In **Criminal proceedings** the police / prosecuting authorities have a legitimate interest in obtaining evidence, including documents, and may request voluntary disclosure from the Diocese / Religious Congregation even though they also have rights to obtain disclosure by means of a court order. Where disclosure is requested, it should only be acceded to without a court order with authorisation from the Data Protection Officer.

2.33. Where the Diocese or Religious Congregation receives a disclosure request in the course of criminal proceedings, the receiving Safeguarding Coordinator should immediately refer it to the relevant Data Protection Officer, who may wish to seek legal advice. This legal advice should be obtained either through the Diocesan or Congregational Insurance Officer, or for dioceses/congregations supported by CIS, by contacting the in house solicitor at CIS.

Disclosure and Barring Service (DBS Check) information

2.34. The Catholic Church in England and Wales (and associated partner organisations) uses DBS Disclosures as part of its Safer Recruitment process. The Catholic Safeguarding Advisory Service, its authorised Counter-Signatories and those deemed to be "employers" are obligated to adhere to the DBS Code of Practice. This dictates that Disclosure information is only shared "*with relevant persons in the course of their specific duties relevant to recruitment and vetting processes*". In practical terms, this means that Disclosure information is only provided to those who have an entitlement in order to make an appointment or selection decision.

2.35. For the Policy Statement on the Safe Storage, Retention and Handling of Disclosure Information (as required by the DBS), please refer to the **Policy on Secure Storage and Retention of DBS Related Documentation.**

What is the process should a person move parish, Diocese, or take up a DBS eligible role with another Catholic partner organisation?

2.36. If an individual asks for confirmation of their Disclosure number and date of issue (where they have misplaced their Certificate copy), you can supply this information either in writing or verbally once you are satisfied that the individual is who they say they are. This can be established by asking the individual to confirm some basic personal details i.e. date of birth, Parish or Order relevant to the role and Disclosure, 1st line of home address and postcode.

What can you do if you have any queries concerning the circumstances in which DBS Disclosure information can or cannot be shared?

2.37. Please consult the DBS Code of Practice to assess whether your intended disclosure is lawful (if you are required to comply with the code of practice): Code of Practice for Disclosure and Barring Service. If you are still not sure whether you can share information, CSAS may be able to assist but in most situations, you are advised to take separate legal advice before disclosing any information to avoid any potential commission of a criminal offence.

3. Making decisions about information sharing

3.1. Before you share any personal information, you must always consider whether it is appropriate to do so. These decisions are not always straightforward.

Initial considerations

3.2. The safety and welfare of a child or an adult must be the primary consideration when making decisions on whether to share information about the child or adult. Where there is concern that the child has suffered, or is likely to suffer significant harm, the child's safety and welfare must be the overriding consideration. Similarly, where there are concerns about the safety of an adult, their welfare takes precedence and information must be shared where a crime is suspected.

3.3. Where information is shared, those doing so must ensure it is accurate and up-to-date, necessary for the purpose for which they are sharing it, minimised, shared only with those people who need to see it, and shared securely.

3.4. HM Government provides guidance about information sharing (see **Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers, July 2018**).

3.5. In order to assist you in making a decision in relation to information sharing, you should work through the following questions:

Why do you need to share the information?

3.6. If you are asked, or wish, to share information about a person you need to have a clear and legitimate reason to do so if it is to be lawful. You must comply with the law relating to confidentiality, data protection and human rights. Establishing a legitimate purpose for sharing information is an essential part of meeting those requirements.

3.7. Although you need to ensure that you have a legitimate purpose for sharing data, please note that there can be equally significant consequences to not sharing information as there can be for sharing information inappropriately.

Do you need to share information which identifies a living person?

3.8. If information is fully anonymised it can be shared without reference to data protection principles. However, true anonymisation of information is difficult to achieve and, if the information to be shared, when considered alongside other information, enables a living person to be identified it is subject to data protection laws.

What information do you need to share?

3.9. If you have a clear reason to share information about an identifiable individual, you will need to consider what information should be shared.

3.10. You should only share information that is necessary and proportionate to achieve the purpose of supporting the safeguarding and protection of a child or young person or vulnerable adult.

3.11. Only information that is relevant to the purposes of supporting the safeguarding and protection of a child or young person or vulnerable adult should be shared with those who need it.

3.12. Information shared should be adequate for its purpose and of the right quality to ensure that it can be understood and relied upon.

3.13. Information shared should be accurate and up to date and should clearly distinguish between fact and opinion.

Is the information to be shared subject to a duty of confidence?

3.14. Information may be subject to a duty of confidence if it is:

- Information of a private or sensitive nature;
- Information that is not already lawfully in the public domain; and
- Information that has been obtained in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

3.15. There is a significant overlap between the duty of confidence and data protection law. However, the duty of confidence can also apply to information which is not 'personal' and so can apply to information not subject to data protection law.

3.16. The duty of confidence is not absolute and may be overridden where the sharing of confidential information is in the best interests of the individual or in the wider public interest, or if the individual consents to the sharing. This must be considered on a case-by-case basis and, if in doubt, legal advice should be sought.

Do you have consent to share the information?

3.17. Under data protection law, consent is one of the six lawful bases for processing personal information. Where possible you should:

- Be open and honest about what personal information you might need to share and why;
- Seek permission to share personal or sensitive information; and
- Respect the wishes of those who do not give consent to share confidential information.

3.18. You should **not** seek consent if doing so would:

- Place a child or an adult at increased risk of significant harm;
- Prejudice the prevention, detection or prosecution of a serious crime;
- Lead to unjustifiable delay in making enquiries about allegations of significant or serious harm; or
- Prevent your organisation or an individual from seeking legal advice on how to handle a situation or set of circumstances.

Does another lawful basis apply that allows you to share information without consent?

3.19. It is not always necessary to obtain consent in order to share personal information. You may share information without consent if, in your judgement, there is another lawful basis allowing you to share or disclose information without an individual's consent e.g. where the child or

young person's safety or wellbeing may be at risk. In deciding, you must weigh up what might happen if the information is shared against what might happen if it is not.

Is the information being shared appropriately and securely?

3.20. You should take into account the following factors:

- Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection;
- Ensure that you are giving the right information to the right individual - only share information with those who need to know and check out the identity of the person you are talking to;
- Make sure the conversation cannot be overheard;
- Use secure email;
- If using fax, make sure the intended person is on hand to receive the fax;
- Check who will see the information and whether they intend to pass on this information; and
- Comply with all other relevant information security policies and procedures in your organisation and, if applicable, the provisions below on DBS Check information.

Has the information sharing decision been recorded properly?

3.21. It is important to record your information sharing decision. This should include:

- The reason for sharing or reason for not sharing (e.g. there was/was not a clear reason and a legitimate reason to share information). If there was not a clear reason and a legitimate reason, information should not be shared and that decision recorded;
- Whether you had consent to share the information or not – if you do not have consent, whether the information enabled any individual(s) to be identified;
- What information was shared, how, when and with whom; and
- Whether information was retained in line with the applicable records retention policy.

3.22. If, at any stage, you are unsure about how or when to share information you should seek advice. You should also ensure that the outcome of the discussion is recorded.

3.23. More information about making and recording decisions can be found in Part 4 of this Chapter.

Examples

3.24. There are many occasions when information needs to be shared between the different organisations within the National Safeguarding Structure, or shared with organisations outside the Catholic Safeguarding Structure such as Police or Social Services.

3.25. The examples set out below indicate the likely application of relevant rules and good practice but should not be taken as definitive guidance and you should take independent legal advice in relation to your specific situation as required.

<u>Case Example 1: Information sharing where there are child protection concerns</u>

3.26. Where you have reasonable cause to believe that a child or young person **has suffered, or is likely to suffer significant harm**, you must always refer your concerns to Children's Services or Police in line with national policy and your Local Safeguarding Children's Board procedures.

3.27. In some situations, there may be a concern that a child or young person has suffered, or is likely to suffer significant harm, or may be causing significant harm to another child or adult. You may be unsure whether what has given rise to your concern constitutes 'a reasonable

cause to believe'. In these situations, the concern must not be ignored. You should always talk to someone to help you decide what to do – for example, a lead person on safeguarding, another experienced colleague, or the CSAS.

3.28. You should protect the identity of the child or young person wherever possible until you have established a reasonable cause for your belief.

Paul, a nine-year-old, tells his mother that his friend John does not go home after liturgy class because Mr Brown always asks him to help clear up. The child is upset saying that John never walks home with him anymore and seems to be different ... "*I don't think he wants to be my friend anymore*".

Paul's mum has also noticed that John is behaving differently and is more withdrawn. She tries to call John's mum but is not able to contact her. She calls the Parish Safeguarding Representative and says that she is concerned about John but at the same time concerned that she may be misreading the situation.

The Parish Safeguarding Representative calls the Safeguarding Co-ordinator who discusses the situation with the local priest. The Priest can offer clarification. At the present time, John's mum is in hospital. Mr Brown is John's uncle and is looking after John whilst his dad visits his wife.

The Safeguarding Co-ordinator informs Paul's mum that she has made enquiries and there is no cause for concern. The Safeguarding Co-ordinator records the enquiry and her actions.

The processing of personal information in this case, including the sharing between the parish, the diocese and the priest, is in accordance with the data protection principles and there is a valid lawful basis for personal information to be shared, because:

- It is in the legitimate interests of the diocese to carry out this processing to ensure that parishioners are safe and to investigate any potential causes for concern or wrongdoing;
- The information is processed for a limited purpose only, which is to investigate a specific concern; and
- The sharing is adequate, relevant and not excessive. Only enough information to check out/allay the concern is shared.

Case Example 2: Information sharing where there are child protection concerns

The Police approach a Diocese requesting information about a youth worker in the Diocese against whom an allegation has been made. A parent alleges she saw him drinking in a pub with several young people under the age of 18. She claims he was flirting with some of the young girls, buying them drinks and offering to drive them home, whilst over the limit.

The Police have the names of some of the young people involved. They have asked for their contact details. This information can be provided to the Police (subject to the Police submitting their request in writing with sufficient information to enable the data requested to be identified and to satisfy you that not disclosing the data would prejudice the police's investigations).

The sharing of personal information with the Police is in accordance with the data protection principles and there is a valid lawful basis for the sharing, because:

- The sharing of information is necessary for the police to carry out their functions to investigate potential crimes (sexual activity with children and drink driving) and there are exemptions in the Data Protection Act 2018 to allow for disclosure of personal data where it is necessary for the prevention or detection of crime;

- The information is processed for a limited purpose only, which is to locate the individuals at risk and for child protection; and
- The sharing is adequate, relevant and not excessive. Only the contact details are shared, which is sufficient for the Police to continue their investigation.

Case Example 3: Information sharing in relation to an allegation of child abuse

3.29. There are occasions when CSAS is contacted by people seeking advice on where to go, or what to do with a concern.

CSAS receives a call from an individual in relation to an incident of alleged child abuse by a volunteer within the Catholic Church.

CSAS listens to the concern, notes the details and passes the information on to the appropriate Diocesan Safeguarding Office for them to refer as appropriate to the local statutory authority.

The sharing of personal information with the appropriate Diocese (and on to the appropriate statutory authority) is in accordance with the data protection principles and there is a valid lawful basis for the sharing, because:

- It is in the legitimate interests of the diocese and in the public interest to carry out this processing to ensure that its parishioners are safe and to comply with the Diocese's legal obligations regarding safeguarding. There is also a substantial public interest in preventing and detecting any potential criminal or unlawful wrongdoing and carrying out safeguarding activities. Depending on the nature of the allegations, it may also be necessary to share the information to protect an individual's vital interests (although this lawful basis only applies to very serious situations where there is a genuine risk to life or health);
- The information is processed for a limited purpose only, which is child protection; and
- The information is adequate, relevant and not excessive. The information which is shared is sufficient for the local Safeguarding Office to proceed.

Case Example 4: Information Sharing to Protect an Adult

CSAS receives a call from an individual concerned about their elderly mother. The mother had reported to her daughter that a priest called at her home and touched her in an inappropriate manner, which could constitute a sexual assault.

The mother is in her eighties, lives alone, has mental capacity and can make informed decisions. She is adamant that she does not want to involve the police or social services but is concerned about other elderly people who the priest may visit.

CSAS informs the daughter that her mother had the right not to inform the police/social services and that her consent would be required for this to happen. This is different from child protection allegations where there is a duty to inform the police. If the mother refuses to take matters further in relation to reporting the incident to the police/social services then her wishes should be respected.

Respecting the individual's rights to self-determination and ensuring the safety of the vulnerable are however not incompatible. The Church has a responsibility to consider other adults with whom the priest has contact and may need to take appropriate action. This may include discussing the situation with the Bishop and/or with the statutory agency without divulging personal information of the mother/daughter.

CSAS suggests that the mother may benefit from talking to the Safeguarding Co-ordinator, who can provide information on the options available. CSAS gives information about the Diocesan Safeguarding Office and the name and contact details of the Safeguarding Co-ordinator. Limited information about the allegations, including the name of the priest, is also shared with the Bishop. This sharing is in accordance with the data protection principles and there is a valid lawful basis for the sharing, because:

- It is in the legitimate interests of the diocese to ensure that its clergy and staff follow correct pastoral procedures and ensure that parishioners' well-being and safety is addressed. There is also a substantial public interest in preventing and detecting any potential criminal or unlawful act;
- The information would have been processed for limited purpose, which is the protection of adults; and
- The information shared is adequate, relevant and not excessive. In this case, it must be sufficient information for the Bishop to consider options, but there is no need to provide personal data identifying the mother or daughter, unless they consent to it.

Case Example 5: National 'Alerts' – sharing information to ensure nationally agreed standards are upheld

3.30. The Catholic Church in England and Wales requires individuals entering its jurisdiction to provide a testimonial of suitability to the Bishop or Congregational Leader before they undertake any active ministry. There are times when people come to the UK and begin active ministry without presenting a testimonial of suitability. Sometimes this means that they are undertaking active ministry in a number of Dioceses or Religious settings. When this comes to light the individual is required to cease active ministry until a testimonial of suitability is received and accepted.

3.31. A problem may arise when the whereabouts of the individual concerned is not known.

It has come to CSAS's attention that a cleric from overseas is undertaking work in the UK without a 'testimonial of suitability'. His/her current whereabouts and contact details are unknown. To clarify the situation the following email alert is sent to all Catholic Safeguarding Co-ordinators:

> *Testimonial of Suitability*
> *We are trying to contact Fr Joe of the xxxxx order in the United States – if you have his contact details or know his whereabouts please let CSAS know at your earliest convenience.*

This sharing of information is in accordance with the data protection principles and there is a valid lawful basis, because:

- It is the legitimate interests of CSAS and of the wider Catholic Church to carry out this processing in order to ensure that only appropriate checked individuals can carry out certain activities and tasks within the Church;
- The information is processed for a limited purpose only, which is to locate the individual in question; and
- The information shared is adequate, relevant and not excessive. Only enough information to identify the individual has been shared. Where CSAS knows more about a particular situation, the sharing can be even more limited. For instance, if Fr Joe is known to be living in London, the alert would only be sent to the Westminster and Southwark co-ordinators.

Alerts in relation to other circumstances, such as where there are legitimate concerns about an individual, may also be sent. However, the content must not include negligent statements or be discriminatory in any way.

Case Example 6: Sharing Information to ensure safeguarding best practice is maintained and is consistent throughout the Catholic Church in England and Wales

3.32. The National Catholic Safeguarding Commission (**NCSC**) has the responsibility to ensure that standards are met and policies implemented (see *Safeguarding with Confidence* p 36 -37).

CSAS is commissioned by the NCSC to undertake, or to commission external organisations to undertake on its behalf, quality assurance exercises into safeguarding arrangements in Dioceses and Safeguarding Commissions. This involves the sharing of personal data with CSAS.

The sharing of personal data is in accordance with the data protection principles and there is a valid lawful basis for the sharing, because:

- It is in the legitimate interests of the Diocese and Commissions to share this information to verify that their procedures are robust and fit for purpose to ensure compliance with safeguarding and other legal obligations;
- The information is processed for a limited purpose, which is for CSAS to carry out quality assurance exercises to ensure adherence with national standards in respect of safeguarding policies and procedures; and
- The information shared is adequate, relevant and not excessive. It is sufficient to enable CSAS to undertake its quality assurance work.

CSAS is commissioned by the NCSC to gather and report on anonymised data for reporting in the NCSC annual report and to inform quality assurance exercises and the development of policy and procedure. Data protection law does not apply to truly anonymised data (i.e. data where no individual is identifiable), and so there are no data protection issues.

If CSAS needed to process personal data in order to create anonymised data sets, then this processing would be in accordance with the data protection principles because:

- It is in the legitimate interests of CSAS and the NCSC to process the data to create the anonymised data as part of its reporting processes;
- Any personal data would be processed for a very limited purpose, which is to enable anonymised reporting on an annual basis of various demographic data; and
- The personal data processed would be adequate, relevant and not excessive. It would be limited to the data required to produce anonymous data in the areas identified by the NCSC for public reporting.

Case Example 7: Request to confirm someone's Disclosure & Barring Service check

There are circumstances when a request to confirm an individual's DBS status is received.

This may arise when the Safeguarding Office has previously DBS-checked an individual for their Church role and that individual is now looking to work or volunteer with an entirely separate body (for example with another Catholic charity).

Whilst the individual may have been DBS checked for their existing Church role, as the information is being sought post disclosure and after the recruitment process concluding, the **signed written consent** of the individual concerned must be provided prior to any information being shared.

The DBS Code of Practice states that only confirmation of the disclosure number, the issue date and the level at which the DBS disclosure was processed (i.e. Standard or Enhanced) can be provided.

It is important to check that the individual to whom you are providing the information is indeed an authorised representative of the requesting organisation.

The sharing of information is in accordance with data protection law because the written consent from the individual has been obtained. Without such consent, there would be no lawful basis for sharing the information and so the sharing would not be permitted by data protection law.

Case Example 8: Appointment of independent investigators, assessors, review panel members

3.33. An independent assessor, investigator or review panel may be commissioned for the purposes of informing the making of recommendations or decisions where concern remains about an individual. This might involve seeking assistance from statutory agencies where they hold information, interviewing witnesses, the victim(s) /complainants, the accused and others who can provide information as to the alleged incidents or other relevant information.

When statutory authorities have withdrawn from the investigative process, for whatever reason, but concerns about an individual remain, a diocese or religious congregation might need to commission an independent person for the specific purpose of investigating or an assessment.

On conclusion of this process, CSAS might need to convene a panel for reviewing the recommendations made by Safeguarding Commissions to Bishops and/or Religious Leaders. To conduct an investigation, assessment or review panel it will be necessary to share information with independent persons outside of the Church safeguarding structures and, where necessary, with CSAS.

This sharing of information with independent investigators / assessors is in accordance with the data protection principles and there is a valid lawful basis, because:

- It is in the legitimate interests of the Church, CSAS and the various commissions to carry out this processing to ensure not just that any safeguarding issues are dealt with but also to ensure that pastoral procedures have been followed and any necessary training requirements / disciplinary measures are carried out. The processing may also be necessary for the establishment, exercise or defence of legal claims and/or to investigate, detect or take steps in relation to unlawful and/or dishonest acts;
- The personal data is processed for limited purposes, which are to protect the young, those at risk, or those who are otherwise vulnerable; and
- The processing is adequate, relevant and not excessive. It must be sufficient for Safeguarding Commissions to make recommendations and Bishops and Religious Leaders to make decisions about the future role of individuals about whom there are concerns. Wherever possible, consideration should be given to only sharing anonymised information.

In these situations, it is important to put in place an agreement with the independent investigator / assessor which clearly sets out what information will be shared and for what purposes. It should also specify any security measures which must be taken to protect personal information.

Case Example 9: Sharing information overseas

3.34. Often situations arise where it is desired to send information overseas to other dioceses or religious orders.

The Safeguarding Coordinator receives an allegation of abuse from a parishioner about a priest from overseas who had been ministering in the parish until his return to his country of origin last year. The Safeguarding Coordinator encourages the parishioner to refer the allegation to the police so that they can liaise with Interpol in respect of the police investigation.

The police decide to not investigate the allegations but, because concerns remain, the Safeguarding Coordinator wants to share information with the priest's superior in his country of origin. This information is shared to ensure that the priest's superior can take any necessary action to prevent potential harm to other parishioners.

The sharing of information is in accordance with the data protection principles and there is a valid lawful basis, because:

- It is in the legitimate interests of the dioceses in the UK and overseas to share this information to ensure that appropriate measures can be taken if required to keep parishioners safe and to take any necessary disciplinary action. Depending on the nature of the allegations, there may be a requirement to share information under safeguarding rules. The processing may also be necessary for the establishment, exercise or defence of legal claims and/or to investigate, detect or take steps in relation to unlawful and/or dishonest acts;
- The personal data is processed for limited purposes, which are to protect the young, those at risk, or those who are otherwise vulnerable; and
- The sharing of personal data is adequate, relevant and not excessive. It should be sufficient to ensure the priest's superior is aware of the allegations and can put any necessary measures in place;

Data protection law contains specific rules in relation to transferring personal data outside the European Economic Area (**EEA**). Depending on where the data is being transferred to, the country in question may be approved as having adequate safeguards in place in respect of personal data and the transfer can be made without further formalities. Alternatively, the transfer is permitted due to the information being provided being of a limited nature, not being part of a repetitive arrangement, being necessary for the compelling legitimate interests pursued by the diocese, and the transfer being risk assessed and appropriate safeguards being put in place prior to the transfer.

No data should be transferred outside the EEA without the approval of the Data Protection Officer, who will consider any need for legal advice.

Further information

3.35. Below are links to guidance which may help you in deciding whether or not to share information:

- General Data Protection Regulation 2016
- Data Protection Act 2018
- Data Sharing Code of Practice (Information Commissioner's Office – to be updated by the ICO in due course)
- Data Sharing Checklists (Information Commissioner's Office – to be updated by the ICO in due course)

- HM Government - Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers (July 2018)
- Human Rights Act 1998
- Care and Support Statutory Guidance issued under the Care Act 2014 and the Social Services and Wellbeing (Wales) Act 2014
- The Cumberlege Commission Report – Safeguarding with Confidence, 2007
- Code of Canon Law

4. Governance Issues

4.1. As well as compliance with the legal issues set out in Part 2 above, organisations must ensure that they have appropriate governance measures in place. This will ensure that decisions are made and recorded appropriately, and that information is handled and retained securely.

The Information Sharing Agreement

4.2. The Information Sharing Agreement is a document that partner organisations/groups within the National Safeguarding Structure sign, demonstrating their commitment to promoting best practice in information sharing. It is a way of promoting a 'one church approach' where partner organisations demonstrate their commitment to responsible and effective communication for the protection of the young, those at risk and the vulnerable, a commitment to respect for the rights of all and for the law.

4.3. If an organisation has signed the Information Sharing Agreement, it does not mean personal data can be freely shared with that organisation. Each time that personal data needs to be shared, the Information Sharing Protocol document must be completed to demonstrate that the data can legitimately be shared and on what ground (see below).

4.4. The Information Sharing Agreement is required:

- To support individuals in the decisions they take to share information, which reduces the risk of harm to children and young people and promotes their well-being;
- To ensure the Catholic Church in England and Wales responds to safeguarding matters in a timely and appropriate manner; and
- To enable the Catholic Church in England and Wales to have confidence knowing that the 'Church' will respond to safeguarding matters appropriately, putting the best interest of the young, those at risk and the vulnerable before the interest of the institution.

4.5. There are risks associated with both sharing and not sharing information, but the risks can be mitigated by informed and considered information sharing decisions. Adhering to key principles can help to make good information sharing decisions.

The Information Sharing Protocol

4.6. The Information Sharing Protocol is intended to safeguard the welfare of the young, those at risk and the vulnerable in our midst by ensuring that information sharing is done safely, legally and appropriately.

4.7. The Cumberlege Commission Report (2007) highlighted the need for a 'One Church Approach' to safeguarding. Adhering to the protocol will demonstrate consistency of safeguarding best practice.

4.8. The objectives of the Information Sharing Protocol are to:

- Encourage the appropriate sharing of information;
- Identify the legal basis for information sharing; and
- Help protect partner organisations from wrongful use of personal data;

4.9. Once completed, the protocol sets out the purpose of the sharing, the legal basis for sharing, and the terms on which the information can be used once it is shared.

4.10. The protocol should not be used as a substitute for obtaining legal advice to address specific circumstances and issues however, nor should it supplant the detailed guidance issued by relevant statutory bodies and the Information Commissioner's Office. It is recommended that you seek independent legal advice at an appropriate stage to ensure your Diocese, Religious Congregation or organisation has in place all the necessary policies and procedures to comply with the relevant rules, and that those policies and procedures are sufficiently robust and consistent with your existing internal operational structures and policies.

Transparency

4.11. Data protection law generally requires organisations to provide information to individuals about how their data will be processed. This is often achieved by means of a **privacy notice**.

4.12. A privacy notice should be issued to any person making contact with CSAS, the NCSC or other safeguarding offices across England and Wales, explaining what they can expect to be done with their personal information when they raise a concern or use safeguarding services.

4.13. Reassurance that the information will be shared only with people who need to know in order to take action to intervene and protect the child or adult should be given. Reassurance about the security of records and the security of the information sharing process and record keeping should be given with a clear explanation that the General Data Protection Regulation and the Data Protection Act 2018 will be observed.

4.14. Giving reassurance about the timing of interventions and feedback to the person raising a concern will assist in managing the process.

Appropriate Policy Document

4.15. Under the Data Protection Act 2018, it is a requirement for organisations to put in place an appropriate policy document in order to process special categories of personal data or data relating to criminal convictions or offences in some circumstances.

4.16. An appropriate policy document must set out how the organisation complies with the requirements of data protection law, including complying with the data protection principles. CSAS has developed a template appropriate policy document which organisations can develop and adapt for use where necessary.

Retention and destruction of information

4.17. Under data protection law, personal data should be kept for no longer than is necessary for the purpose for which it is held. However, data protection law does not contain any prescriptive time limits for holding personal data.

4.18. The table below sets out the suggested retention periods for each type of information which may be held relating to safeguarding issues:

Name	Retention period	Rationale for retention period
Cases/situations that although reported to the Catholic Church, do not involve case management by the Church. All records relating to enquiries and actions in respect of individuals that are referred to other organisations and there is no ongoing safeguarding case management role for the Church. These might include allegations against individuals in different denominations and parishioners who require welfare support from statutory authorities.	1 year or for as long as necessary to respond to any ongoing queries e.g. from the authority that the information has been passed to, if this is later. A summary record including date, name of individual, and action taken is to be retained indefinitely.	The person against whom allegations have been made holds no role within the Church, either as an office holder or a volunteer. If referred to another body, they will hold their own more detailed safeguarding record. The summary record is retained to demonstrate that the referral was received and acted on.
All records relating to information about an individual referred to the safeguarding office that does not constitute a safeguarding matter or require any ongoing action.	A summary record including date, name of individual, and action taken is to be retained indefinitely where the person concerned is a member of clergy and for 12 months for all others.	The information does not constitute a safeguarding matter or require any further action. The summary record is retained to demonstrate that the information was received and considered.
Case files in the name of alleged perpetrator that are likely to include, but not restricted to: CM1 – referral form Case recording log Chronology of significant events Case summaries (excluding final summary when main file records are being deleted) Letters/emails/texts/other electronic messaging sent and received Minutes of meetings IRA2 Risk Assessment Agreement and any agreement between commissioned assessor/investigator and person being assessed/investigated Safeguarding Plans Risk Information Framework	For clergy and religious, 85 years from date of birth, or date of death if later. At the end of the relevant period, a summary record of the case file will be retained indefinitely. For all other church roles e.g., volunteers, office holders, 25 years from the date their role ceases or at least 6 years after the date of death of the accused person if this is sooner. At the end of these retention periods, a summary record of the case file will be retained until the 85th birthday of the accused person. The summary record should include:	Clergy and Religious generally have a lifelong relationship with the Church and dioceses and religious congregations have vicarious liability for their actions whilst within the Church, even after they have left the Church. We know that people often do not tell the Church about alleged abuse for many years after it is said to have occurred. For these reasons, full case files concerning religious and clergy are to be kept until the accused person's 85th birthday or death if later, and summary files are to be kept indefinitely. In respect of other roles, the Limitation Act 1980

Reports e.g. risk assessment, psychological, psychiatric, investigative, National review template forms Legal and restricted information which must be kept in a separate section of the file.	Name of accused: DOB: DOD: Role: Date of ordination(employment): Movement between dioceses/religious congregations: Summary of safeguarding issues/convictions etc: Record of DBS checks/other checks (e.g. testimonials): Summary of actions taken by the Church: Name of alleged victim(s): DOB of alleged victims:	provides for a limitation period of 3 years for personal injury claims from the date of the incident, or from the claimant's 18th birthday if the incident occurred prior to that date. However, Judges have an unfettered discretion under the Limitation Act to allow a claim to proceed outside of these timescales. We know that people often do not tell the Church about alleged abuse for many years after it is said to have occurred. For this reason, we keep full files until 25 years after the role ceases and summary files until the 85th birthday of the accused person.
<u>Parish or other event/activity related records. Records are likely to include but are not restricted to:</u> PHOTO 1 – Parental consent to use of images Case 2 – Approval of events form Case 4 – Parental consent for an activity Case 5 – Session recording sheet *Case 6 – Incident report form	3 years after event/activity ceases. <u>*Case 6</u> - Incident involving an adult – 3 years from date of incident - Incident involving a child – 21 years from date of incident	Records need to be kept in case of incidents occurring at events. The general limitation period for personal injury claims is 3 years from the date of incident or 3 years from a child's 18th birthday, if a child has been injured. Incidents may not be reported contemporaneously, so these records need should be kept for 3-years post-event/activity in case a claim is made. Case 6 Where an incident has occurred, the record should be kept for the full limitation period. NB If a safeguarding file is opened in relation to an incident, the IRF may be transferred onto that file and the retention

		period for that file will apply.
<u>Personnel related files and records. Records are likely to include, but are not restricted to:</u> *Electronic entries on the CSAS DBS Database DBS 1 – Volunteer registration form DBS 2 – Volunteer reference form **DBS 3 – ID verification form ***DBS 4 – Safeguarding self-declaration form DBS 5 – Withdrawal of consent to undertake DBS online Update Service checks DBS 9 – Confidentiality Agreement for individuals handling DBS Disclosure information and accessing the national database DBS 10 – Counter-signatory agreement between Catholic dioceses/religious congregations in relation to the provision of DBS Disclosures DBS 11 – Request for a new counter-signatory to be added to the CSAS Registered Body account DBS 12 – Request for removal of a counter-signatory from the CSAS Registered Body account DBS 13 – Ebulk user exit form DBS 14 – Ebulk end-user agreement Blemished DBS Disclosure risk assessment form CASE 1 – Written Agreement for volunteers which indicates that they have read and understood their job description and agree to adhere to national safeguarding procedures	10 years and 1 day after person leaves their role. *Where a case file is opened, the entries on the DBS Database e.g. date of check and existence of a risk assessment, should be recorded on the case file before the electronic record is destroyed **Existing DBS 3 forms can be destroyed when a new form is completed. ***Existing DBS4 forms can be destroyed when a new Disclosure application has been completed and any queries about Disclosure content and prior self-disclosure have been resolved. Once a recruitment (or other relevant) decision has been made, do not keep certificate information for any longer than is necessary e.g. to allow for the consideration and resolution of any disputes or complaints. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access must prevail.	We know that people often do not tell the Church about concerns or abuse for many years after it is said to have occurred. For this reason, we retain records on volunteers and safeguarding roles for a ten-year period after they leave their role, or at least six years following death if this is sooner.

Case 9 – Declaration that the volunteer has understood the safeguarding procedures Testimonials of suitability Form 1 – Supervision Agreement Form 3 – Record of supervision Form 4 – Record of individual case discussion Form A – Preparation by role holder for appraisal Form B – Preparation by supervisor for appraisal Form C – Annual appraisal summary		
DBS15 – Information security incident form (data breach)	6 years after date of incident	Data Subjects affected by an information security breach have up to 6 years from the date of the breach to bring a claim.

Appendix:

CSAS Information Security Policy for Disclosure and Barring Services Including Handling, Access, Usage, Storage, Retention & Disposal of Disclosures and Disclosure Information

Policy statement

As an organisation using the Disclosure and Barring Service (**DBS**) to help assess the suitability of applicants for positions working with children, young people and adults at risk, CSAS complies fully with the **DBS Code of Practice** regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information. It also complies fully with its obligations under the **General Data Protection Regulation,** the **Data Protection Act 2018,** and other relevant legislation.

This policy applies to CSAS and its agents within the safeguarding structures of dioceses and religious congregations, across the Catholic Church of England and Wales, who process Disclosure Applications and may hold information relating to that processing locally.

All DBS applicants using the CSAS registered body will be issued with a DBS specific Privacy Notice and will be required to sign an application form in relation to the processing of their application agreeing to the use of their personal information for the DBS check.

1. Objectives of the Information Security Policy

To ensure that:

- DBS related information is afforded adequate protection in accordance with its sensitivity. It is recognised that information about criminal proceedings is not permitted to be processed under the General Data Protection Regulation unless UK domestic law permits processing. UK domestic law allows for processing of this information in certain circumstances within the Data Protection Act**;**
- Information held can be relied upon for completeness and accuracy;
- Information is used, maintained, stored and disposed of in compliance with all applicable laws, regulations and contractual obligations;
- Access to information and associated IT systems is only permitted to persons who have a business need for such access and such access is restricted to the purposes associated with their role;
- Any processing of personal data will be carried out in accordance with the provisions of the General Data Protection Regulation and the Data Protection Act.

2. Classification

CSAS regards Disclosures and Disclosure information as confidential and requires that agents of the Registered Body adhere to the requirements set out in this policy document. Disclosures and Disclosure related information must be stored securely and only accessed by individuals who need to know the content.

Information transmitted verbally or electronically should be subject to the same level of protection as physical documents to ensure the confidentiality, security and integrity of the information. Confidential documentation must not be stored on unsecured shared network drives or mobile devices. Confidential information should not be discussed in public places and confidential or sensitive information should not be left on answerphone messages. When transmitting Disclosure related information electronically e.g. via email, documents should be encrypted and confidential information should not be included in the subject line or body of the email text.

When no longer required, Disclosure related information must be securely destroyed in accordance with the timescales set out in the record retention schedule.

3. Handling and Access

In accordance with Section 124 of the Police Act 1997 (as amended), Disclosure information must only be passed on to those who are authorised to receive it in the course of their duties. CSAS maintains a record of all those to whom Disclosures or Disclosure information has been disclosed and recognises that it is a criminal offence to pass this information on to anyone who is not entitled to receive it.

Only named individuals, having signed the CSAS DBS Confidentiality Agreement and received appropriate training, are approved to process applications, carry out the ID verification process and permitted access to Disclosure documentation.

All applications to the DBS must be counter-signed. Counter-signatories are approved by the CSAS Lead Signatory and cannot countersign applications until:

- their own DBS application has been approved by the DBS, and they have been given a counter-signatory number;
- they have undertaken mandatory counter-signatory training with CSAS:
- they have signed the CSAS DBS Confidentiality Agreement.

E-Bulk users will be set up with the correct permissions according to the user's designated role of Master Disclosure Manager, Disclosure Manager or ID Verifier and appropriate training will be provided. Master Disclosure Managers and Disclosure Managers will be required to sign the CSAS e-Bulk End User Agreement before access to the system is granted.

Access to Disclosure e-Bulk schema results is limited to Master Disclosure Managers and Disclosure Managers. ID Verifiers will not have access to e-Bulk schema results or be able to export information.

Only the e-Bulk service provider shall have access to the e-Bulk system for the purposes of maintenance and upgrade. Third party requests for access to the system will need to be approved by the Facilities and Operations Manager (via CSAS), who acts as the gateway for all information security requests, which are dealt with in accordance with this policy and all other relevant policies and procedures. Third parties who are granted access to information to which this policy applies will be required to sign the CSAS DBS Confidentiality Form before access is granted. Their access will be the minimum required for the duration to carry out the task requested of them.

The DBS may, while provisioning Registered Bodies to use the e-Bulk service, provide access to, or enable them to acquire knowledge of, the DBS's technical and process specifications, systems, and other information of or with respect to security and technical measures which may not be accessible or known to the public. Such information must be protected from inappropriate access and unauthorised disclosure. Any requests for disclosure of information relating to e-Bulk, including any made under the Freedom of Information Act should be referred to CSAS (for referral to the DBS) before disclosure is considered. Requests for the release of any documentation issued by the DBS and classified as "restricted" must not be disclosed by anyone other than the DBS.

4. Usage

Disclosure 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 or where another lawful basis or bases for processing exists.

5. Storage and Retention

Disclosure information must not be kept on an applicant's personnel file and must always be kept separately and securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are authorised to see it as part of their duties.

Once an appointment (or other relevant) decision has been made, CSAS and its agents do not keep Disclosure information for any longer than is necessary. The retention period for all DBS related documentation is set out in the CSAS record retention schedule. If it is considered necessary to keep Disclosure information for longer than the time period set out in the record retention schedule, we will consult the DBS and consider the rights of the data subject under the General Data Protection Regulation, the Data Protection Act 2018 and the Human Rights Act 1998 before doing so. Throughout this time, the requirements set out above regarding the safe storage and strictly controlled access will continue to apply. Any retention beyond that set out in the record retention schedule will be limited to the minimum period necessary.

CSAS and its agents must not make or keep any copy or representation of the contents of a Disclosure. CSAS and its agents will, however, keep a record, on the national database, of the date of issue of a Disclosure, the name of the data subject, the type of the Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the appointment decision taken. The national database holds a record of all DBS applications and is checked by agents of CSAS across England and Wales, before a new DBS application is made, to ensure that applications are not made where an appropriate DBS Disclosure Certificate already exists.

E-Bulk schema results are not to be printed out, nor retained electronically other than within the e-Bulk system. The e-Bulk system will automatically retain information for a period of 6 months following a Disclosure result.

6. Retention of records

The timescales for the retention of DBS related records are set out in the CSAS safeguarding record retention schedule.

Safeguarding self-declaration form (SSD)

The SSD will be retained by the safeguarding office that is processing the DBS application.

ID verification form

The ID verification form, which the applicant completes for the purposes of identity verification at interview stage and is presented at that time by the applicant along with original documentary evidence of identity, is to be retained by the appropriate countersignatory or safeguarding office that is processing the DBS application.

In the event of the application being withdrawn before completion, then the ID verification form can be destroyed by secure means as outlined in section 7 below.

ID evidence – photocopies of documents

The photocopies of original identity documentary evidence (taken originally at interview or ID verification stage are submitted by the ID verifier to the safeguarding office that is processing the application and are retained by that office until the Disclosure process has been completed. If there are questions about accuracy of content of the DBS Disclosure, then the ID documents should be retained until the matter is resolved and then disposed of securely.

Registered Body handling of the Disclosure Certificate

Where the Registered Body or its agents need to see the original copy of the DBS Disclosure Certificate (e.g. to risk assess disclosure information), the original Disclosure Certificate must be returned to the applicant by secure post e.g. signed for or tracked, once the risk assessment process has concluded.

7. Disposal

Once the retention period has elapsed, CSAS and its agents will ensure that any Disclosure information is permanently and securely destroyed when no longer needed by dust shredding machines (or other equally destructive method) so it is not readable/useable for any purpose. While awaiting destruction, Disclosure information will not be kept in any unsecure receptacle (e.g. waste bin or confidential waste sack).

The e-Bulk system will automatically purge the Disclosure information and any supporting information (such as ID verification) after 6 months.

8. Acting as an Umbrella Body

Before acting as an Umbrella Body (one which counter-signs applications and receives Disclosure information on behalf of other employers or recruiting organisations connected to the Catholic Community in England and Wales,) CSAS will take all reasonable steps to satisfy ourselves that the organisations that we act as an Umbrella Body for will handle, use, store, retain and dispose of Disclosure information in full compliance with the DBS Code of Practice 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 to use or adapt for this purpose.