January 2012

# Information Sharing Protocol

## Agreement & Best Practice Guidance for Safeguarding within the Catholic Church of England & Wales

Carol Parry
Catholic Safeguarding Advisory Service

NCSC
National Catholic Safeguarding Commission

**CONTENTS:**

## INTRODUCTION

The Catholic Church in England and Wales is committed to promoting a culture of safeguarding. In order 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 crucial.

Sharing information has many benefits, in particular enabling organisations to cooperate thus helping to ensure the young and the vulnerable are given the protection they need. We are also mindful that sharing information presents risks if done insensitively and/or unlawfully.

This Protocol is intended to be a simple practical guide to help all involved in safeguarding within the Catholic Church in England and Wales to develop the confidence to make good decisions in relation to information sharing. The Information Sharing Agreement 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 and the vulnerable.

## CONTEXT

The Catholic Church's national safeguarding structure comprises of a number of organisations and groups between which information, when appropriate, is shared. Partner organisations include: Dioceses, Religious Congregations, Catholic voluntary groups/organisations, Catholic Safeguarding Advisory Service and the National Catholic Safeguarding Commission.

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.

This Protocol provides a framework that will facilitate appropriate sharing of personal and/or sensitive information between partner organisations within the National Safeguarding Structure and also with the appropriate Statutory Agencies. It is recommended that each organisation which is a signatory to this Information Sharing Agreement should obtain the contact details for its Local Authority Designated Officer (LADO) and Police Child Protection Unit and should keep them readily available for those who may be called upon to use them.

**The aim of this Information Sharing Protocol is to** safeguard the welfare of the young and the vulnerable in our midst.

**The objectives of this Information Sharing Protocol are to:**

- Encourage the appropriate sharing of information.
- Identify the legal basis for information sharing.
- Increase awareness and understanding on key issues relating to information sharing.
- Provide a guide on how to share personal information lawfully.
- Help protect partner organisations from wrongful use of personal data.
- Introduce the Information Sharing Agreement.

**To this end the Protocol:**

- Sets out the principles of information sharing.
- Sets out the legal obligations, rules and regulations which organisations and individuals must follow when sharing information.
- Takes into account the legal requirements including:
  - Common Law Duty of Care;
  - Data Protection Act 1998;
  - The Human Rights Act 1998;
  - The Freedom of Information Act 2000.
- Is informed by:
  - No Secrets: Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse (Department of Health 2000);
  - Framework of Code of Practice for Sharing Information (Information Commissioner's Office 2007);
  - Data Sharing Code of Practice (Information Commissioner's Office 2011);
  - Information Sharing – Guidance for Practitioners and Managers (HM Government 2008).
- Establishes the means by which information sharing practices between the various parts of the safeguarding structure can be monitored.
- Applies to all information shared between partner organisations including electronically and manually held records.

**QUESTIONS & ANSWERS**

**What do we mean by Information Sharing?**

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 protocol is primarily aimed at information that is shared between organisations and groups within the National Safeguarding Structure. The principles also apply to sharing information with statutory agencies.

**What are the benefits of adhering to an Information Sharing Protocol?**

The Cumberlege Commission Report (2007) highlighted the need for a 'one church approach' to safeguarding – adhering to this protocol will demonstrate consistency of safeguarding best practice.

The Protocol offers clarity on when and how information can be shared legally, in line with best safeguarding practice.

**What is an Information Sharing Agreement?**

The Information Sharing Agreement is a document which partner organisations/groups within the Catholic Safeguarding Structure sign up to adhering to key principles of the Information Sharing Protocol.

**Why is an Information Sharing Agreement required?**

The Information Sharing Agreement will help to:

- protect the young and the vulnerable from abuse and harm.
- ensure the Catholic Church in England and Wales responds to safeguarding matters in a timely and appropriate manner.
- enable the whole church to have confidence knowing that the 'Church' will respond to safeguarding matters appropriately, putting the best interest of the young and the vulnerable before the interest of the institution.
- ensure individuals are not constrained by uncertainty about what information they can/cannot share.

**How do you know when, and what information to share?**

There can be significant consequences to not sharing information as there can be for sharing information. The following questions will help in deciding whether or not to share information, what information is appropriate to share and what you need to record.

**1. Is there a clear and legitimate purpose for sharing the information?**

If you are asked, or wish, to share information about a person you need to have a good reason to do so if it is to be lawful. You have to comply with the law relating to confidentiality, data protection and human rights. Establishing a legitimate purpose for sharing information is an important part of meeting those requirements. **See Appendix 4**

**2. Does the information enable a living person to be identified?**

If information is anonymised it can be shared. 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. **See Appendix 3**

**3. Is the information confidential?**

Confidential information is:

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

4. **Do you have consent to share 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;
- respect the wishes of those who do not give consent to share confidential information.

**NB** You may share information without consent, if in your judgement the lack of consent is overridden in the public interest. In making a decision you must weigh up what might happen if the information is shared against what might happen if it is not.

In some circumstances you should not seek consent if doing so would:

- place a child or vulnerable 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.

**5. Is the information shared appropriately and securely?**

- You should only share information that is necessary to achieve the purpose.
- Only share information with those who need to know.
- Check out the identity of the person you are talking to.
- Make sure the conversation cannot be overheard.
- As far as possible make sure that the information is accurate and up to date.
- 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.

**6. Has the information sharing decision been recorded properly? See Appendix 1**

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

- The reason for sharing or not sharing
- The purpose of sharing the information
- What information was shared, how and with whom.

**What about Criminal Record Bureau Disclosure (CRB Check) information?**

The Catholic Church in England and Wales (and associated partner organisations) use CRB Disclosures as part of its Safer Recruitment process. CSAS, its authorised Counter-Signatories and those deemed to be "employers" are obliged to adhere to CRB 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.

For the Policy Statement on the Safe Storage, Retention and Handling of Disclosure Information (as required by the CRB), please refer to the CSAS online policy manual: http://www.csasprocedures.uk.net/chapters/p_safer_recruit.html#storage

**What is the process if a person moves parish, Diocese, or takes up a CRB eligible role with another Catholic partner organisation?**

A key benefit of a single Registered Body (CSAS) for the Catholic Church of England & Wales, is the ability to minimise the need for numerous Church CRB checks should a person move parish, Diocese, or work with a Religious Order or a Catholic Charity *(with whom CSAS has an Umbrella Body Agreement).*

**NB** In the event that 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 indeed 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/Disclosure, first line of home address and postcode.

For detailed guidance on how to proceed in these circumstances, please refer to the CSAS online policy manual: http://www.csasprocedures.uk.net/chapters/p_safer_recruit.html#specific

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

You can contact CSAS for assistance. This will ensure that the Church does not breach Data Protection legislation or CRB Code of Practice, which could jeopardise the CRB services within the national safeguarding structure.

**PRACTICE GUIDANCE – KEY PRINCIPLES**

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 facilitates information being shared for specific lawful purposes, or where appropriate consent has been obtained. It does not give licence for unrestricted access to information between partner organisations.

**1. SHARING INFORMATION WITHOUT CONSENT**

Organisations must be aware that an individual may withdraw consent to processing their personal information. In such instances processing can only continue where an applicable condition as set out in the Data Protection Act (DPA) 1998 Schedule 2 (personal data) and /or Schedule 3 (sensitive personal data) applies. **See Appendix 3**

Partner organisations should not assume that non personal information is not sensitive information.

In order to disclose personal data (where consent to share is withheld or gaining consent is not appropriate or possible) the DPA 1998 requires that at least one condition of Schedule 2 must be met. Where the information is personal and sensitive then at least one condition in both Schedules 2 and 3 must be met. Fairness and lawfulness must be considered alongside the conditions in Schedules 2 and 3. **See Appendix 3**

Where there is a statutory obligation to disclose personal data then consent of the data subject is not required: wherever possible the data subject should be informed that the obligation exists.

Where consent is used as a form of justification for disclosure, the data subject must be informed of their right to withdraw consent at any time.

Specific procedures apply where the data subject is not able to give informed consent due to age (Gillick Competency) or where the individual has a condition that means that they do not have the capacity to give informed consent:
http://www.nspcc.org.uk/inform/research/questions/gillick_wda61289.html

## 2. ADHERENCE TO THE DATA PROTECTION PRINCIPLES:

Partner Organisations must ensure that all information is:

- Fairly and lawfully processed;
- Processed for limited purpose;
- Adequate, relevant and not excessive;
- Accurate and kept up to date;
- Not kept longer than necessary;
- Processed in line with a given individual's rights;
- Kept secure;
- Not transferable to other countries without adequate protection. (CSAS advice should be sought when sharing information abroad).

## 3. COMPLIANCE/MONITORING

Partner organisations accept responsibility for auditing compliance with the Information Sharing Agreement.

Dioceses will be audited against National Information Sharing Quality Standards by the Catholic Safeguarding Advisory Service (CSAS), on behalf of the National Catholic Safeguarding Commission (NCSC).

### 3.1 Written policy:

Partner organisations will have a written policy for the retention and disposal of information.

### 3.2 Responsibility for staff:

Each partner organisation is responsible for ensuring that staff are aware and comply with the obligations to protect confidentiality and a duty to disclose information only to those who have a right to it.

Each partner organisation ensures that any staff accessing information under the Information Sharing Agreement is fully aware of their responsibilities to maintain the security and confidentiality of the personal information.

All partner organisations have a responsibility to ensure their staff are trained to a level which enables them to undertake the information sharing tasks confidently, efficiently and lawfully.

### 3.3 Information Sharing & Condition of Employment

Each partner organisation includes within the written conditions of employment that employees agree to abide by the rules and policies in relation to the protection and use of personal data.

## 4. INDIVIDUAL RESPONSIBILITY

Every individual working for partner organisations:

- is responsible for the safekeeping of any information they obtain, handle, use or disclose;
- knows how to obtain, use, and share information they legitimately need in order to do their job;
- has an obligation to take steps to validate the authorisation of another before disclosing any information requested under this protocol;
- must uphold principles of confidentiality;
- must be aware that any violation of privacy or breach of confidentiality is unlawful and is a disciplinary matter.

## 5. REVIEW ARRANGEMENTS

The agreement will be formally reviewed periodically by CSAS subject to revised legislation or national guidance. Any signatory can request an extraordinary meeting at any time.

Each partner organisation must ensure that revisions to the protocol and to the Information Sharing Agreement are communicated to all staff in a timely fashion.

**INFORMATION SHARING AGREEMENT**

We the undersigned agree to adhere to the key principles laid out in the Information Sharing Protocol thereby sharing information with our partner organisations legally, appropriately and efficiently.

Name of Organisation: _____

Name: _____

Position: _____

Signature: _____

Signed on behalf of the Organisation /Trust /Trustees *(please circle as appropriate)*

**Please return to:**

Catholic Safeguarding Advisory Service
Queensway House
57 Livery Street
Birmingham
B3 1HA

**APPENDIX 1**

| **INFORMATION SHARING REQUEST/DECISION FORM** | |
|---|---|
| Name of organisation requesting information: | |
| Name and position of person requesting information: | |
| Date of request: | |
| Reason:<br>*(state whether or not there is a clear and legitimate reason to share information)* | |
| Purpose:<br>*(explain the legitimate reason)* | |
| Decision:<br>*(disclose/not disclose)* | |
| Data sharing decision made by:<br>*(Name and position)* | |
| Any specific arrangements re retention/deletion of data: | |
| Signed: | |
| Date: | |

**APPENDIX 2**

**SEVEN GOLDEN RULES** (Information Sharing Guidance 2008 - HM Government)

1. The Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about a living person is shared appropriately.

2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest.

5. Base your information sharing decisions on considerations of the safety or well-being of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

**APPENDIX 3**

**DATA PROTECTION LAW**

**SCHEDULE 2**

**Conditions relevant for the purposes of the first principle: Processing of any personal data**

At least **one** of the following conditions must be met whenever you process **personal data:**

1. The data subject has given their consent to the processing.

2. The processing is necessary:
    a) for the performance of a contract to which the data subject is a party;
    *OR*
    b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary for the administration of justice, or for exercising statutory, or other public functions.

6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the individual to whom the data relates.

*The Data Subject is a living individual to whom personal data relates.

* A Data Controller is the individual who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

**APPENDIX 3**

**DATA PROTECTION LAW**

**SCHEDULE 3**

**Conditions relevant for the purposes of the first principle: Processing of sensitive personal data**

At least one of the following conditions must be met whenever you process **sensitive personal data:**

1. The data subject has given his/her explicit consent to the processing of the personal data.

2. The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

3. The processing is necessary to protect the vital interests of:
    a) data subject (in a case where the individual's consent cannot be given or reasonable obtained);
    b) another person (in the case where the consent by or on behalf of the data subject has been unreasonably withheld).

4. The processing is carried out by a not for profit organisation and does not involve disclosing of personal data to a third party, unless the individual consents otherwise and it is carried out with appropriate safeguards for the rights and freedoms of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing is necessary for the purpose of, or in connection with, any legal proceedings such as:
    a) obtaining legal advice;
    *OR*
    b) establishing, exercising or defending legal rights.

*The Data Subject is a living individual to whom personal data relates.

* A Data Controller is the individual who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

## APPENDIX 4

### CASE EXAMPLES OF INFORMATION SHARING THAT ARE APPROPRIATE AND LAWFUL

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.

### CASE EXAMPLE 1: Information sharing where there are child protection concerns

Where you have reasonable cause to believe that a child or young person **may be suffering or be at risk of suffering significant harm,** you must always consider referring your concerns to Children's Services or Police in line with national policy and your Local Safeguarding Children's Board procedures.

In some situations there may be a concern that a child or young person may be suffering, or be at risk of suffering significant harm, or of 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 – a lead person on safeguarding, another experienced colleague or CSAS.

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 – 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 Coordinator who discusses the situation with the local priest. The Priest is able to 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 Coordinator informs Paul's mum that she has made enquiries and there is no cause for concern.

The Safeguarding Coordinator noted the enquiry and her actions.

The sharing of information is:

- Fairly and lawfully processed – there is a legitimate reason for processing.
- Processed for limited purpose – to check out a concern.
- Adequate, relevant and not excessive – only enough information to check out/allay concern.

**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 a number of young people under the age of 18. She claims that 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 and have asked for their contact details. This should be provided to the Police.

The sharing of information is:

- Fairly and lawfully processed – there is a legitimate reason for processing the investigation of at least 2 potential crimes (sexual activity with children and drink driving).
- Processed for limited purpose – to locate the individuals at risk and for child protection.
- Adequate, relevant and not excessive – sufficient for the Police and the Local Authority Safeguarding team to make an informed decision.

**CASE EXAMPLE 3: Information sharing in relation to an allegation of child abuse**

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 will listen to the concern, note details and pass information on to the appropriate Diocesan Safeguarding Office for them to refer as appropriate to the local statutory authority.

The sharing of information is:

- Fairly and lawfully processed – there is a legitimate reason for processing.
- Processed for limited purpose – child protection.
- Adequate, relevant and not excessive – sufficient for the local Safeguarding Office to proceed.

**CASE EXAMPLE 4: Information sharing to protect a vulnerable 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 good mental facilities, and is able to make informed decisions. The mother is adamant that she does not want to involve the police or social services but was concerned about other elderly people who the priest may visit.

The daughter wants to know if she should report the incident to the police.

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.

Respecting the individual's rights to self determination and ensuring the safety of the vulnerable are however not incompatible.

CSAS suggested the mother may benefit from talking to the safeguarding coordinator who would provide information on the options available. If the mother refused to take matters further in relation to reporting the incident to the Police/Social Services then her wishes should be respected.

The Church has a responsibility to consider other vulnerable 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 gave information about the Diocesan Safeguarding Office and the name and contact details of the Safeguarding Coordinator.

The mother agreed to see the Safeguarding Coordinator; agreed to the Bishop being informed but refused permission to report the incident to the Police. If the mother had refused permission to inform the Bishop then information could still be shared as:

The sharing of information is:

- Fairly and lawfully processed – there is a legitimate reason for processing.
- Processed for limited purpose – protection of vulnerable adults.
- Adequate, relevant and not excessive – sufficient for the Bishop to consider options (with no details of the mother/family given).

**CASE EXAMPLE 5: National 'Alerts' – Sharing information to ensure nationally agreed standards are upheld**

The Catholic Church in England and Wales require clergy or religious entering their 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 situation has to be rectified - the individual is required to cease active ministry until a Testimonial of Suitability is received and accepted.
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…

**CSAS response:** In order to clarify the situation an email alert is sent to all Catholic Safeguarding Coordinator/Officer to the effect:

"*Testimonial of Suitability"*

*"We are trying to contact Fr Joe of the xxx order in the United States – if you have his contact details please let CSAS know as soon as possible".*

This statement respects the data protection principles – in particular:

- Fairly and lawfully processed – there is a legitimate reason for processing.
- Processed for limited purpose – to locate the individual.
- Adequate, relevant and not excessive – only enough information to identify individual and the issue in question.

**CASE EXAMPLE 6: Sharing information to ensure safeguarding best practice is maintained and is consistent throughout the Catholic Church in England and Wales**

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

CSAS is commissioned by the NCSC to undertake "quality" audits into safeguarding arrangements in Dioceses covering the three primary areas of:

- Casework and recording practice;
- Induction, support and training;
- Safer Recruitment practice.

The sharing of information is:

- Fairly and lawfully processed – there is a legitimate reason for processing.
- Processed for limited purpose – to ensure adherence to safeguarding policy/ procedures.
- Adequate, relevant and not excessive – sufficient to check out compliance to policy/procedures.

**CASE EXAMPLE 7: Request to confirm someone's Criminal Record Bureau check**

There are circumstances when a request to confirm an individual's CRB status is received. This may arise in 2 particular circumstances:

1. The Safeguarding Office has CRB checked an individual for their Church role and that person is now looking to work/volunteer with an entirely separate body (for example with another Catholic charity). The other organisation is seeking to use "portability".

   In these cases, **the signed written consent** of the individual to whom the CRB Disclosure relates is essential before any information is supplied.

   Please refer to the specific "Portability" Guidance contained within the online CSAS Procedures Manual for full guidance on how to proceed and what information can be shared. See Chapter 4.2 (Safer Recruitment Practice including CRBs); section 20 – Specific Topics or Circumstances including changes of Role; Portability and DP Act: http://www.csasprocedures.uk.net/chapters/p_safer_recruit.html#specific

2. St. Vincent de Paul Society contacts the Safeguarding Office requesting confirmation in relation to the CRB status of an individual that works for them.

   Whilst the individual may have been CRB checked for that role, as the information is being sought post Disclosure and subsequent to the recruitment process concluding, **the signed written consent** of the individual concerned must be provided to the Counter-Signatory prior to any information being shared.

   The CRB Code of Practice dictates that only confirmation of the Disclosure number; the issue date and the level at which the CRB Disclosure was processed (i.e. Standard or Enhanced) is 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:

- Fairly and lawfully processed – written consent is obtained.

**CASE EXAMPLE 8: Preliminary Enquiry**

The NCSC preliminary enquiry protocol is the procedure for an internal enquiry of apparent inappropriate conduct. This follows the completion of criminal investigations where a concern remains or it may be in relation to conduct which does not amount to a crime but where the position of an accused person within the Church needs to be considered.

Where a concern remains, an independent person (that is independent of the Diocese or religious congregation) is appointed to carry out such enquiries as appropriate, seeking assistance from the statutory agencies where they hold information, as well as interviewing witnesses/the victim(s) or complainant(s)/the accused and others who can provide information as to the alleged incidents or other relevant information.

The independent person (paid or voluntary) is instructed by the 'trust/organisation' concerned. Before an independent person is instructed to carry out the enquiry he/she must be approved by CSAS. Therefore CSAS needs to know the nature of the enquiry to be carried out to ensure the investigator has the right skill mix to undertake the task to a high professional standard.

The independent enquiry function respects the data protection principles:

- Fairly and lawfully processed – there is a legitimate reason for processing.
- Processed for limited purpose – protection of the young or the vulnerable.
- Adequate, relevant and not excessive – sufficient for the Safeguarding Commission to make an informed decision.

**BIBLIOGRAPHY**


1. Data Protection Act, 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents

2. Data Sharing Code of Practice 2011
http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.pdf

3. *Framework of Code of Practice for Sharing Information* (Information Commissioner's Office, 2007)
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/ico_information_sharing_framework_draft_1008.pdf

4. *Information Sharing: Guidance for practitioners and managers*, DCSF, HM Government, 2008
https://www.education.gov.uk/publications/eOrderingDownload/00807-2008BKT-EN-March09.pdf

5. The Human Rights Act, 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

6. The Freedom of Information Act, 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

7. *No Secrets: Guidance on developing and implanting multi-agency policies and procedures to* protect vulnerable adults from abuse, Department of Health, 2000
http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4074540.pdf

8. *The Cumberlege Commission Report - Safeguarding with Confidence,* 2007
http://www.cathcom.org/mysharedaccounts/cumberlege/index.htm