National Safeguarding Information Sharing Protocol

This Protocol should be read in conjunction with the:

- Information Sharing Overview
- General Privacy Notice for CSAS
- Privacy Notice for DBS checks
- National Safeguarding Record Retention Schedule
- Policy and Procedure relating to Right of Access Requests

Contents

1. Introduction and Context
2. Information Sharing Questions and Answers
3. Seven Golden Rules for Information Sharing
4. Information Sharing Agreement Key Principles

Appendix 1: Information Sharing Agreement

Appendix 2: Information sharing Request/Decision Form

Appendix 3: Data Protection Law

Appendix 4: Case Examples

Bibliography

1. Introduction and Context

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.

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 insensitivity 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.

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 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, those at risk and the vulnerable, a commitment to respect for the rights of all and for the law.

Context

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.

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 special categories of information (formerly sensitive personal data) and/or information relating to criminal convictions and offences (the latter category now being dealt with separately under data protection legislation) between partner organisations within the National Safeguarding Structure, the appropriate Statutory Agencies and other relevant organisations. It is recommended each organisation that is a signatory to the Information Sharing Agreement obtains the contact details for its Designated Officer (formerly known as the LADO)/Designated Adult Safeguarding Manager (DASM)) and Police Child Protection Unit and keeps 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, those at risk and the vulnerable in our midst.

The objectives of this Information Sharing Protocol are to:

- Encourage the appropriate sharing of information;
- Provide a basic understanding of the restrictions on sharing confidential information and the exceptions;
- 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;
- Provide guidance on when to seek legal advice
- 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 guidance on the legal obligations, rules and regulations which organisations and individuals must follow when sharing information;
- Considers the legal requirements including the:
    - Common law duty of care;
    - Common law duty of confidence
    - General Data Protection Regulation 2016;
    - Data Protection Act 2018;
    - The Human Rights Act 1998;
- Is informed by:
    - Data Sharing Code of Practice (Information Commissioner's Office)

  - HM Government - Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers (July 2018);
  - Care and Support Statutory Guidance issued under the Care Act 2014 and the Social Services and Wellbeing (Wales) Act 2014.
- Establishes how information sharing practices between the various parts of the National Safeguarding Structure can be monitored;
- Applies to all information shared between partner organisations including electronically and manually held records.

This 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.

2. Information Sharing Questions and 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 and in line with best safeguarding practice.

What is an Information Sharing Agreement?

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.

Why is an Information Sharing Agreement 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;

- 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.

Who are you likely to share information with?

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 NCSC;
- Children's Social Care Services professional staff;
- Adult Social Care Services professional staff;
- The Police;
- The NSPCC.

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.

What information is it appropriate to share?

Information Sharing: Advice for Practitioners Providing Safeguarding Services (July 2018) states that:

The GDPR and Data Protection Act 2018 do not prohibit the collection and sharing of personal information. They provide a framework to ensure that personal information is shared appropriately. In particular, the Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them. Never assume sharing is prohibited – it is essential to consider this balance in every case. You should always keep a record of what you have shared.

You do not necessarily need the consent of the information subject to share their personal information.

Wherever possible, you should seek consent and be open and honest with the individual from the outset as to why, what, how and with whom, their information will be shared. You should seek consent where an individual may not expect their information to be passed on. When you gain consent to share information, it must be explicit, and freely given. There may be some circumstances where it is not appropriate to seek consent, either because the individual cannot give consent, it is not reasonable to obtain consent, or because to gain consent would put a child or young person's

safety or well-being at risk. Where a decision to share information without consent is made, a record of what has been shared should be kept.

There can be significant consequences to not sharing information as there can be for sharing information. The following questions will help in deciding if to share information and what information is appropriate to share.

- Is there a clear and legitimate purpose for sharing information?
- Does the information enable a living person to be identified?
- Is the information confidential?
- Do you have consent to share the information?
- Where information is confidential to a group e.g. members of a family, have you considered whether there is anyone else from whom agreement should be sought before information is shared?
- Is there sufficient public interest to share the information?
- Are there any other lawful bases that allow you to share the information?
- Are you sharing information appropriately and securely?
- Have you recorded your information sharing decision?

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 must 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.

Does the information enable a living person to be identified?

If information is fully anonymised it can be shared without reference to data protection principles. However, true anonymization 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.

Is the information subject to a duty of confidence?

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.

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.

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 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 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.

In some circumstances 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;
- Prevent your organisation or an individual from seeking legal advice on how to handle a situation or set of circumstances.

Is the information being shared appropriately and securely?

- 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;
- 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;
- Information shared should be adequate for its purpose and of the right quality to ensure that it can be understood and relied upon;
- Information shared should be accurate and up to date and should clearly distinguish between fact and opinion;
- 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;
- 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?

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;
- Whether information was retained in line with the applicable records retention policy.

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.

What about Disclosure and Barring Service (DBS Check) information?

The Catholic Church in England and Wales (and associated partner organisations) uses DBS Disclosures as part of its Safer Recruitment process. CSAS, 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.

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?

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?

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. Seven Golden Rules for Information Sharing

1. The General Data Protection Regulation 2016, the Data Protection Act 2018, the law of confidence and human rights laws are not themselves barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared only where it is appropriate to do so;
2. Be open and honest with the individual (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 from other practitioners or legal advisors if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible;
4. Where possible, share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may share information without consent if, in your judgement, there is good and lawful reason to do so, such as where safety may be at risk or doing so would enable the prevention or detection of crime. You will need to base your judgment on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared;
5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and wellbeing of the individual 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.

Source:- HM Government- Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers (July 2018);

4. Information Sharing Agreement 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.

1. Adherence to the Data Protection Principles

All information sharing is:

- Fairly and lawfully processed and in a transparent manner;
- Processed 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.

1.1 **Fairly and lawfully processed**

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.

Organisations must be aware that an individual may withdraw consent to processing their personal information. In such instances processing can only continue if you are required to retain the information for a different purpose under another lawful basis and it is fair to do so. Lawful bases are set out in Article 6 of the General Data Protection Regulation 2016 (for personal data) and Article 9 of the General Data Protection Regulation and/or Schedule 1 of the Data Protection Act 2018. See Appendix 2: Information Sharing Request/Decision Form. Partner Organisations should not assume that non-personal information is not sensitive information.

1.2 **Sharing information without consent**

To disclose personal data where consent to share is withheld, or gaining consent is not appropriate or possible, the General Data Protection Regulation requires that at least one lawful basis in Article 6 must be met. Where the information is personal and special category or relating to criminal convictions or offences then at least one lawful basis in both Articles 6 and 9 must be met. Fairness and lawfulness must be considered alongside the bases in Articles 6 and 9. See Appendix 2: Information Sharing Request/Decision Form.

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 competent to give informed consent due to their maturity and understanding of the nature of the consent required (Gillick Competency / Fraser Guidelines) or where the data subject is aged 16 or over and has a condition that means that they lack capacity to give informed consent to sharing information. See Gillick Competency and Fraser Guidelines, NSPCC 2009.

1.3 **Restriction on the use of shared information**

All shared information is for a specific, explicit and legitimate purpose; any further uses made of this data may not be lawful or covered by the Information Sharing Agreement.

1.4 **Security**

Each partner organisation is responsible for ensuring that their technical and organisational security measures protect the lawful use of information shared under this protocol and minimises the risk of unauthorised or unlawful processing, accidental loss, destruction or damage.

Information is not transferable to other countries without adequate protection. Full information on when you can and cannot transfer information to other countries is available here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

2. Quality of information

Information needs to be of a standard that is fit for purpose - this means that information should be accurate, up to date, minimised and not kept for longer than necessary as outlined in the DPA principles.

3. Training

Organisations must ensure that staff are trained to a level which enables them to undertake the information sharing tasks confidently, efficiently and lawfully.

4. Compliance/Monitoring

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

The NCSC will commission CSAS or an external organisation to undertake audits of information sharing arrangements and practices across the Catholic Church in England and Wales.

4.1 **Written Policy**

Partner organisations will have a written policy for the retention and disposal of information which demonstrates how they will comply with the DPA principles.

4.2 **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 staff accessing information under the Information Sharing Agreements are fully aware of their responsibilities to maintain the security and confidentiality of the personal information.

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

4.3 **Information sharing and 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.

5. 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 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 may be unlawful and is a disciplinary matter.

6. 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.

Appendix 1: Information Sharing Agreement - see separate document on website

Appendix 2: Information Sharing Request/Decision Form

Information Sharing Request / Decision Form	
Name of organisation requesting information:	
Name and position of person requesting information:	
Date of request:	
Information requested: (type/volume/ sensitivity etc)	
Reason: (there is/is not a clear reason and a legitimate reason(s) to share information)	
Purpose: (explain the legitimate reason(s))	
Decision: (disclose/not disclose)	
Data sharing decision made by: (Name and position)	
Any specific arrangements regarding transfer/retention/deletion of data:	
Signed:	

Date:	

Appendix 3: Data Protection Law

Schedule 2: Lawful Bases Relevant for the Purposes of Article 6 of the General Data Protection Regulation: Processing of any Personal Data

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

(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 (this cannot apply if you are a public authority processing data to perform your official tasks).

Schedule 3: Lawful Bases Relevant for the Purposes of the First Principle: Processing of Special Category Personal Data

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

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that a prohibition on processing of this type of information may not be lifted by the data subject;

(b) 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 in so far as it is authorised by Union or Member State law or a collective

agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) 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;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to certain conditions and safeguards referred to the GDPR;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Organisations need to read these alongside the Data Protection Act 2018, which adds more specific conditions and safeguards:

- Schedule 1 Part 1 contains specific conditions for the various employment, health and research purposes under Articles 9(2)(b), (g), (i) and (j) of the GDPR (set out above);

- Schedule 1 Part 2 contains specific 'substantial public interest' conditions for Article 9(2)(h) (set out above);

- In some cases, you must also have an 'appropriate policy document' in place to rely on these conditions.

Schedule 4: Lawful Bases Relevant for the Purposes of the First Principle: Processing of Personal Data relating to Criminal Convictions and Offences

The General Data Protection Regulation 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 basis set out within that legislation that will permit the necessary processing.

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.

The list of conditions is extensive and each condition is detailed in nature – full details can be found here:

https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted

However, the conditions under Schedule 1 Parts 2 and 3 that are likely to be most relevant for handling information under this Protocol 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 non-for-profit bodies
- Paragraph 33 – legal claims

Appendix 4: Case Examples

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

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

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

Case example 4: Information sharing to protect an adult

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

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

Case example 7: Request to confirm existence of a DBS check

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

Case example 9: Sharing information overseas

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

Case Example 1: Information Sharing Where there are Child Protection Concerns

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 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 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 - 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 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 noted the enquiry and her actions.

The sharing of information was:

- Fairly and lawfully processed - it is in the legitimate interests of the diocese and in the public interest to carry out this processing to ensure that parishioners are safe and to investigate any potential causes for concern or wrongdoing;
- 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 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 can be provided to the Police (subject to the Police providing the correct completed and signed request form beforehand – often called a "DP2" form).

The sharing of information is:

- Fairly and lawfully processed - it is in the legitimate interests of the police for the diocese to carry out this processing - the investigation of at least 2 potential crimes (sexual activity with children and drink driving) – and there are exemptions in the DPA 2018 to allow for disclosures in relation to the prevention and detection of crime;
- 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 would 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 - 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 its 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. It may also be necessary to protect an individual's vital interests (life and death issues) depending on the severity of the allegations;
- Processed for limited purpose - child protection;
- Adequate, relevant and not excessive – sufficient information 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.

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.

CSAS suggested the mother may benefit from talking to the safeguarding co-ordinator 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.

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 gave information about the Diocesan Safeguarding Office and the name and contact details of the Safeguarding Co-ordinator. The mother agreed to see the Safeguarding Co-ordinator; agreed to the Bishop being informed but refused permission to report the incident to the Police. Had the mother refused permission to inform the Bishop then information could still be shared as:

The sharing of information is:

- Fairly and lawfully processed - it is in the legitimate interests of the diocese to carry out the processing 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 wrongdoing;
- Processed for limited purpose - protection of adults;

- Adequate, relevant and not excessive – sufficient information for the Bishop to consider options (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 individuals 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 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: To clarify the situation an email alert is sent to all Catholic Safeguarding Co-ordinators to the effect:

"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 statement respects the data protection principles - in particular:

- Fairly and lawfully processed - it is the legitimate interests and in the public interest for CSAS to carry out this processing – requesting information about an individual – and of the diocese(s) – in sharing relevant information – to ensure that only appropriate checked individuals carry out certain activities and tasks within the Church;
- Processed for limited purpose - to locate the individual;
- Adequate, relevant and not excessive - only enough information to identify individual and the issue in question. Information is also only released to neighbouring dioceses where possible e.g. Fr Joe is known to be living in London so the alert is initially sent to the Westminster and Southwark co-ordinators.

Alerts in relation to other circumstances e.g. where there are legitimate concerns about an individual, can be sent but the content must not include negligent statements or be discriminatory.

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, or to commission external organisations to undertake on its behalf, quality assurance exercises into safeguarding arrangements in Dioceses and Safeguarding Commissions.

The sharing of information is:

- Fairly and lawfully processed - it is in the legitimate interests of the diocese and commissions to share this information to ensure that their arrangements are robust and fit for purpose to ensure compliance with safeguarding and other legal obligations;
- Processed for limited purpose - to ensure adherence to safeguarding policy/ procedures and national standards;
- Adequate, relevant and not excessive - sufficient to check out compliance to policy/procedures.

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.

The sharing of information is:

- Fairly and lawfully processed - there is a legitimate reason for processing (although if the information is fully anonymised the data protection legislation does not apply);
- Processed for limited purpose - to enable anonymised reporting on an annual basis of various demographic data relating to Safeguarding across dioceses and religious congregations in England and Wales; to inform the selection of quality assurance exercises; to inform the development of policy and procedure;
- Adequate, relevant and not excessive - sufficient to report on 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 because:

- The Safeguarding Office has DBS 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 DBS Disclosure relates is essential before any information is supplied;

- St. Vincent de Paul contact the Safeguarding Office requesting confirmation in relation to the DBS status of an individual that works for them;

  Whilst the individual may have been DBS checked for that 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 to the Counter-Signatory prior to any information being shared.

The DBS Code of Practice dictates 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) 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: Appointment of independent investigators, assessors, review panel members

Where an independent assessor, investigator or review panel is commissioned for the purposes of informing the making of recommendations or decisions where concern remains about an individual. This might involve seeking assistance from the 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, and concerns 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 review 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.

The sharing of information is:

- Fairly and lawfully processed - 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;
- Processed for limited purpose –for protecting the young, those at risk or those who are vulnerable;
- Adequate, relevant and not excessive - 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.

Case Example 9: Sharing information overseas

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

The Safeguarding Coordinator received 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 encouraged the parishioner to refer the allegation to the Police so that they could liaise with Interpol in respect of police investigation. The police decided to not investigate the allegations but because concerns remained, the Safeguarding Coordinator wanted to share information with the priest's superior in his country of origin. This information was shared to ensure that the priest's superior could take any necessary action to prevent potential harm to other parishioners.

The sharing of information is:

- Fairly and lawfully processed - 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 ensure parishioners are safe and to take any necessary disciplinary action. There may also be a requirement to share such information under safeguarding rules depending on the allegations made; 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;

- Processed for limited purpose - protecting the young, those at risk or those who are vulnerable;
- Adequate, relevant and not excessive - sufficient to ensure the priest's superior was aware of the allegations and put any necessary measures in place;
- Transferring out of the EEA – depending on the country to which the transfer is being made, the country in question may be approved by the EU Commission 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.

The need for legal advice should be considered if transferring information out of the EEA.

Bibliography

1. **Common Law Duty of Care**:
2. General Data Protection Regulation 2016
3. Data Protection Act 2018
4. Data Sharing Code of Practice (Information Commissioner's Office – to be updated by the ICO in due course)
5. Data Sharing Checklists (Information Commissioner's Office – to be updated by the ICO in due course)
6. HM Government - Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers (July 2018)
7. Human Rights Act 1998
8. Care and Support Statutory Guidance issued under the Care Act 2014 and the Social Services and Wellbeing (Wales) Act 2014
9. The Cumberlege Commission Report – Safeguarding with Confidence, 2007
10. Code of Canon Law