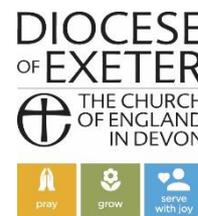


Data Protection with regard to Safeguarding Related Data in the Diocese of Exeter

July 2019



In Summary

- The overall objectives for processing and sharing Safeguarding information are to protect children and adults from abuse, harm or neglect.
- Where it is necessary to process data for the 'Safeguarding of children and of individuals at risk' we have lawful bases for the processing of that data without consent of the data subject.
- Where we have a 'legitimate interest' we can process data without requiring consent.

In Detail

The General Data Protection Regulations introduced by the European Union came into effect in May 2018 and were ratified in law in England and Wales through the Data Protection Act 2018. Whilst there were a few significant considerations with regard to data protection under GDPR there needs to be a recognition that most of what GDPR covers was already expected under the principles of the previous Data Protection Act 1998. With regard to data processed¹ for the purposes of Safeguarding children and adults at risk, there needs to be an understanding of how this data requires different treatment from the general personal data handled by organisations for purposes such as marketing or commerce. The UK government have recognised this important difference and have designated Safeguarding data as a 'special category' of data in the Data Protection Act 2018.

Explicit consent was the highest profile element of the GDPR changes, with little balancing commentary on the subject of other lawful bases for processing such as 'vital interests' and 'legitimate interests' that allow personal data to be processed where consent is not available or appropriate, or not required. This information imbalance led to a large volume of enquiries, with much fear and consternation in parishes about what this means for Safeguarding. 'Vital interests' is where the processing is necessary to protect someone's life. 'Legitimate interests' is where the processing is necessary to fulfil the legitimate interests of the data controller or a third party where it can be shown that the legitimate interests would override the data privacy interests of the data subject on balance. In the Data Protection Act 2018, the UK government have identified the 'Safeguarding of children and of individuals at risk' as in the 'substantial public interest' and the Church of England's Safeguarding Policy (Promoting a Safer Church 2017) commits the Church to the objective of Safeguarding children and adults:

"The Church of England, its archbishops, bishops, clergy and leaders are committed to safeguarding as an integral part of the life and ministry of the Church.

¹ Processing, in relation to information or data, means obtaining, recording or holding the information or data, or carrying out any operation or set of operations on the information or data, including sharing

Safeguarding means the action the Church takes to promote a safer culture. This means we will promote the welfare of children, young people and adults, work to prevent abuse from occurring, seek to protect those that are at risk of being abused and respond well to those that have been abused. We will take care to identify where a person may present a risk to others, and offer support to them whilst taking steps to mitigate such risks.

The Church of England affirms the 'Whole Church' approach to safeguarding... The Church will take appropriate steps to maintain a safer environment for all and to practice fully and positively Christ's Ministry towards children, young people and adults; to respond sensitively and compassionately to their needs in order to help keep them safe from harm."

Therefore we can justifiably consider Safeguarding as a legitimate interest for the lawful basis of processing in the Church.

When considering if the data you are processing qualifies as the special category of Safeguarding data, the definition from the Data Protection Act 2018 is where the processing of this data is necessary for the purposes of:

- protecting an individual from neglect or physical, mental or emotional harm, or
- protecting the physical, mental or emotional well-being of an individual,
- where the individual is aged under 18, or
- aged 18 or over and at risk.

Considering the processing of Safeguarding data in the Diocese of Exeter and its parishes, the special category of data basis of lawful processing will be particularly applicable for disclosed information that will affect the safety or well-being of an individual (whether that individual is the data subject or not) and Safeguarding records relating to ex-offenders or persons known to present a risk. While recognising the lawful bases that exist, there has to be consideration given to the balance between an individual's rights and freedoms and the need to process this data, and the impact of this is assessed. By example, if we were to require consent from the data subjects in such instances then their lack or refusal of consent could put children or adults at risk of harm and could prevent the investigation of a crime and any subsequent prosecution; the balance of interests therefore means that obtaining consent would not be appropriate and we have a lawful basis for processing without consent.

Consent is still an appropriate basis for processing the personal data we might request from an individual during the course of Safeguarding activities in the Diocese of Exeter in a very limited set of circumstances (e.g. Confidential Declaration forms and DBS applications where consent is required under the DBS Code of Practice). With consent obtained we do not have to consider the over-riding of an individual's interests.

Safeguarding data is processed and shared in the Church of England, the Diocese of Exeter and all its parishes and associated bodies on the following lawful bases in compliance with the legislation:

Lawful basis for GDPR Article 6 (personal) data:

EU Data Protection Regulation 2016 (GDPR) The Data Protection Act 2018	Legitimate Interest (Art 6f) - to undertake tasks and duties which are in the legitimate interest of the bodies and officials which make up the Church of England.
---	--

Lawful basis for GDPR Article 9 (special category) data:

EU Data Protection Regulation 2016 (GDPR) The Data Protection Act 2018	Substantial Public interest (Art 9 (2) (g) Schedule 1, Part 2 (18)
---	---

Lawful bases for GDPR Article 10 (criminal offence) data:

EU Data Protection Regulation 2016 (GDPR)	Substantial public interest (Art 9 (2) (g))
England and Wales -The Data Protection Act 2018	Schedule 2 paragraph 11 – processing is necessary for the exercise of a protective function.

Legitimate Interest Assessment

We have a specific purpose with a defined benefit.	The consideration of Safeguarding information in order that we can identify and investigate any potential wrongdoing, inappropriate behaviour, or unlawful conduct and put in place a safer way of working across the Church of England.
The processing is necessary to achieve the defined benefit.	Without a thorough and comprehensive understanding of the detail of the matters raised, we cannot take steps to ensure that we have provided the most appropriate Safeguarding response.
The purpose is balanced against, and does not override, the interests, rights and freedoms of data subjects.	There is the risk of significant and/or serious harm to others if unsuitable individuals are in or may be placed in positions of authority and responsibility and/or roles where they are trusted by others or are in regular contact with Church bodies. This risk is greatest where relevant information is not processed or shared in order to identify and/or properly address concerns. The duty to protect individuals from harm supports their rights and freedoms.

Safe and Secure Storage

The Data Protection Act 1998 required personal data to be stored securely and this requirement is maintained by the GDPR and the Data Protection Act 2018. As Safeguarding data is a special category of data we have to recognise the associated sensitivity of that data and need to pay extra attention to the secure storage and safe handling of this data. The measures are not prescribed, but we are directed to implement appropriate technical and

organisational measures to ensure a level of security appropriate to the risk. Note that this is not limited to electronic security and consideration must be given to how and where information is stored and who has access. When thinking about who has access, consider who has a 'need to know' in order to protect individuals from harm?

The Church of England have assessed acceptable mechanisms for transferring or sharing Safeguarding information, as listed below:

Automated	Data transfer from system to system
	Automated data transfer via secure network
Courier	Paper documents sent or received by courier
	Encrypted removable media e.g. cd / dvd / memory stick
Email	Email address is confirmed and accurate. Limit use of "cc"; use of "bcc" and only where necessary for those who need to know to be included.
	Password protected documents
Encryption	Encrypted email solution (Egress etc) or where email is encrypted and used only within the organisation (Office 365 Outlook)
	Documents are encrypted using 7zip or similar software, where there is no cost to recipients
Hand delivered/Post	By known persons only
	Encrypted removable media
	Media/ documents in tamper-free sealed envelope/ box/ container and fully addressed
	Tracked post - Special Delivery/Recorded Signed for)
Manual system transfer	Manual transfer by authorised individuals only
	Upload or download via secure link to secure system or site
	Documents on secure app/website
Text	On encrypted mobile phones only or where data is segregated from users' personal data
	Mobile phone numbers are accurate and confirmed
	Data is transferred to other secure locations and deleted from senders' phone when necessary

The following transfer mechanisms are not acceptable under the guidance:

- Fax
- Normal mail (i.e. without being recorded/signed for)
- Any other method not listed in the table above

Data Retention

Safeguarding related data has a justifiable retention period that is typically longer than in other areas of processing personal data. There are many reasons for this, but they include consideration of the need to be able to investigate non-recent allegations of abuse and

identify potential victims of non-recent abuse, and the legal requirement to be able to provide evidence to inquiries such as IICSA. Based on the latest advice from the Church of England and the IICSA inquiry team, here are suggested data retention periods to aid compliance with any future requests for Safeguarding related data.

Data Type	Retention Period
Safeguarding Records Relating to Persons of Interest (i.e. offenders, ex-offenders, persons presenting a risk to others)	70 years after last contact with the individual concerned.
Safeguarding Records Relating to Persons of Concern (i.e. incident records, disclosures, victim/survivor details)	70 years after last contact with the individual concerned.
Records that Relate to Safeguarding Concerns/Allegations about Church Officers (paid or unpaid [excluding clergy ²]), including details of how these are handled, followed up, actions taken, decisions reached and eventual outcome	75 years after employment/appointment ceases.
Confidential Declaration forms	Where no information is self-disclosed: 7 years from the date of the appointment decision to which they relate. Where information is self-disclosed on the form: 75 years after employment/appointment ceases.
DBS (Disclosure & Barring Service) Disclosures /disclosure certificates	6 months from the date of the appointment decision to which they relate. <i>(Certificate number and issue date are permitted to be recorded in Safer Recruitment records for the appointment, but no more.)</i>
E-Bulk Disclosure Cover Sheets	6 months from the issue date of the related DBS disclosure.
Parish Information Log Sheets and other records that evidence adherence to the Safer Recruitment process (i.e. records of receipt of references, outcome of interviews, notification of appointment decision)	75 years after employment/appointment ceases.
Safeguarding Training Records	75 years after employment/appointment ceases.
Personnel Records Relating to Paid Workers	75 years after employment ceases.
Home Visit Records	50 years after the last visit to the person.

² Retention of data and records relating to clergy is covered by the House of Bishops' policy on Personal Files Relating to Clergy

Records of any Children’s Activities, (i.e. Sunday School/Junior Church/Youth Club/Choirs) and related safety risk assessments	50 years after the activity ceases.
Records of any Activities Specifically Aimed at Vulnerable Adults (i.e. Bereavement Groups, Dementia Cafes) and related safety risk assessments	50 years after the activity ceases.
Safeguarding Communications Distribution Lists	6 months after notification that appointment to relevant role has ceased.

Questions

If you have any data protection questions specific to Safeguarding data, then please email the Diocesan Safeguarding Team: SafeguardingEnquiry@exeter.anglican.org

If you have broader questions about data protection then you can email the Data Protection Team: DataProtection@exeter.anglican.org