Retention and destruction of information

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

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

Name	Retention period	Rationale for retention period
Cases/situations that although reported to the Catholic Church, do not involve case management by the Church. All records relating to enquiries and actions in respect of individuals that are referred to other organisations and there is no ongoing safeguarding case management role for the Church. These might include allegations against individuals in different denominations and parishioners who require welfare support from statutory authorities.	1 year or for as long as necessary to respond to any ongoing queries e.g. from the authority that the information has been passed to, if this is later. A summary record including date, name of individual, and action taken is to be retained indefinitely.	The person against whom allegations have been made holds no role within the Church, either as an office holder or a volunteer. If referred to another body, they will hold their own more detailed safeguarding record. The summary record is retained to demonstrate that the referral was received and acted on.
All records relating to information about an individual referred to the safeguarding office that does not constitute a safeguarding matter or require any ongoing action.	A summary record including date, name of individual, and action taken is to be retained indefinitely where the person concerned is a member of clergy and for 12 months for all others.	The information does not constitute a safeguarding matter or require any further action. The summary record is retained to demonstrate that the information was received and considered.
Case files in the name of alleged perpetrator that are likely to include, but not restricted to: CM1 – referral form Case recording log Chronology of significant events	For clergy and religious, 85 years from date of birth, or date of death if later. At the end of the relevant period, a summary record of the case file will be retained indefinitely.	Clergy and Religious generally have a lifelong relationship with the Church and dioceses and religious congregations have vicarious liability for their actions whilst within the Church, even after they

Case summaries (excluding final summary when main file records are being deleted) Letters/emails/texts/other electronic messaging sent and received Minutes of meetings IRA2 Risk Assessment Agreement and any agreement between commissioned assessor/investigator and person being assessed/investigated Safeguarding Plans Risk Information Framework Reports e.g. risk assessment, psychological, psychiatric, investigative, National review template forms Legal and restricted information which must be kept in a separate section of the file.	For all other church roles e.g., volunteers, office holders, 25 years from the date their role ceases or at least 6 years after the date of death of the accused person if this is sooner. At the end of these retention periods, a summary record of the case file will be retained until the 85th birthday of the accused person. The summary record should include: Name of accused: DOB: DOD: Role: Date of ordination(employment): Movement between dioceses/religious congregations: Summary of safeguarding issues/convictions etc: Record of DBS checks/other checks (e.g. testimonials): Summary of actions taken by the Church: Name of alleged victim(s): DOB of alleged victims:	have left the Church. We know that people often do not tell the Church about alleged abuse for many years after it is said to have occurred. For these reasons, full case files concerning religious and clergy are to be kept until the accused person's 85th birthday or death if later, and summary files are to be kept indefinitely. In respect of other roles, the Limitation Act 1980 provides for a limitation period of 3 years for personal injury claims from the date of the incident, or from the claimant's 18th birthday if the incident occurred prior to that date. However, Judges have an unfettered discretion under the Limitation Act to allow a claim to proceed outside of these timescales. We know that people often do not tell the Church about alleged abuse for many years after it is said to have occurred. For this reason, we keep full files until 25 years after the role ceases and summary files until the 85th birthday of the accused person.
<u>Parish or other event/activity related records. Records are likely to include but are not restricted to:</u> PHOTO 1 – Parental consent to use of images	3 years after event/activity ceases.	Records need to be kept in case of incidents occurring at events. The general limitation period for personal injury claims is 3

Case 2 – Approval of events form Case 4 – Parental consent for an activity Case 5 – Session recording sheet *Case 6 – Incident report form	<u>*Case 6</u> - Incident involving an adult – 3 years from date of incident - Incident involving a child – 21 years from date of incident	years from the date of incident or 3 years from a child's 18th birthday, if a child has been injured. Incidents may not be reported contemporaneously, so these records need should be kept for 3-years post-event/activity in case a claim is made. Case 6 Where an incident has occurred, the record should be kept for the full limitation period. NB If a safeguarding file is opened in relation to an incident, the IRF may be transferred onto that file and the retention period for that file will apply.
<u>Personnel related files and records. Records are likely to include, but are not restricted to:</u> *Electronic entries on the CSSA DBS Database DBS 1 – Volunteer registration form DBS 2 – Volunteer reference form **DBS 3 – ID verification form ***DBS 4 – Safeguarding self-declaration form DBS 5 – Withdrawal of consent to undertake DBS online Update Service checks DBS 9 – Confidentiality Agreement for individuals handling DBS Disclosure	10 years and 1 day after person leaves their role. *Where a case file is opened, the entries on the DBS Database e.g. date of check and existence of a risk assessment, should be recorded on the case file before the electronic record is destroyed **Existing DBS 3 forms can be destroyed when a new form is completed. ***Existing DBS4 forms can be destroyed when a new Disclosure application has	We know that people often do not tell the Church about concerns or abuse for many years after it is said to have occurred. For this reason, we retain records on volunteers and safeguarding roles for a ten-year period after they leave their role, or at least six years following death if this is sooner.

information and accessing the national database DBS 10 – Counter-signatory agreement between Catholic dioceses/religious congregations in relation to the provision of DBS Disclosures DBS 11 – Request for a new counter-signatory to be added to the CSSA Registered Body account DBS 12 – Request for removal of a counter-signatory from the CSSA Registered Body account DBS 13 – Ebulk user exit form DBS 14 – Ebulk end-user agreement Blemished DBS Disclosure risk assessment form CASE 1 – Written Agreement for volunteers which indicates that they have read and understood their job description and agree to adhere to national safeguarding procedures Case 9 – Declaration that the volunteer has understood the safeguarding procedures Testimonials of suitability Form 1 – Supervision Agreement Form 3 – Record of supervision Form 4 – Record of individual case discussion Form A – Preparation by role holder for appraisal Form B – Preparation by supervisor for appraisal	been completed and any queries about Disclosure content and prior self-disclosure have been resolved. Once a recruitment (or other relevant) decision has been made, do not keep certificate information for any longer than is necessary e.g. to allow for the consideration and resolution of any disputes or complaints. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access must prevail.	

Form C – Annual appraisal summary		
DBS15 – Information security incident form (data breach)	6 years after date of incident	Data Subjects affected by an information security breach have up to 6 years from the date of the breach to bring a claim.