SAFEGUARDING RETENTION POLICY

Version 1.1

Version History

Version	Summary of amendments/changes	Published Date
Version 1.0	Document Created	Dec 2024
Version 1.1	Updated: Introduction, Pupose, Types of Records Covered, Retention Principles & Standard Periods, Storage, Security & Access Controls, Disposal & Destruction of Records Added: Legal & Regulatory Framework, Data Protection Principles & Lawful Bases for Safeguarding Data, Jurisdiction-Specific Retention Considerations, Storage, Data Sharing, Multi-Agency Working & Cross-Border Transfers, Data Subject Rights & Requests, Data Breach Management & Reporting, Training, Audit & Compliance Monitoring, Policy Review & Version Control, Reporting Concerns or Complaints about Data Handling	Dec 2025

Contact Information

IGA Office	info@igauk.com / 0345 319 7000
Safeguarding Team	safeguarding@igauk.com
Kylie Downie	safeguarding@igauk.com

Contents

1. Introduction
2. Purpose
3. Scope
4. Legal & Regulatory Framework
5. Data Protection Principles & Lawful Bases for Safeguarding Data
6. Types of Records Covered
7. Retention Principles & Standard Periods
8. Jurisdiction-Specific Retention Considerations
9. Storage, Security & Access Controls
10. Data Sharing, Multi-Agency Working & Cross-Border Transfers
11. Data Subject Rights & Requests
12. Disposal & Destruction of Records
13. Roles & Responsibilities
14. Data Breach Management & Reporting
15. Training, Audit & Compliance Monitoring
16. Policy Review & Version Control
17. Reporting Concerns or Complaints about Data Handling

Introduction

IGA is committed to protecting the safety, welfare, and rights of all gymnasts, coaches, staff, volunteers, and associated personnel. As part of this commitment, IGA recognises the critical importance of appropriately managing and retaining sensitive safeguarding and welfare-related records — including child protection, health and medical information, consent forms, incident reports, and related documentation — in compliance with applicable data-protection and safeguarding legislation across all jurisdictions in which it operates.

This Safeguarding & Data Retention Policy provides a clear and consistent framework for how IGA and its affiliated clubs collect, store, share, retain, and dispose of safeguarding and welfare-related data. It ensures that records are managed in a way that respects individual privacy and dignity, supports the welfare and protection of gymnasts, and meets legal, regulatory, and moral obligations in England & Wales, Scotland, Northern Ireland, the Republic of Ireland, and the Channel Islands.

The policy applies to all IGA organisations, clubs, committees, staff, volunteers, and anyone acting on behalf of IGA. It covers all types of safeguarding and welfare-related records, including but not limited to: child protection files, consent and information-sharing forms, health or medical records, incident and concern reports, training and compliance logs, personnel vetting documentation, and communications relating to safeguarding matters.

The primary objectives of the policy are to:

- Protect the dignity, privacy, and confidentiality of individuals — athletes, staff, and others — whose sensitive information may be recorded.
- Ensure records are kept only as long as necessary, in line with legal, regulatory, and safeguarding best-practice standards.
- Provide clear guidance on lawful bases for handling safeguarding data, and safeguard data security, storage, and access controls.
- Enable responsible data-sharing and multi-agency cooperation when required, while maintaining data protection and confidentiality.
- Establish oversight, accountability, and transparent procedures for retention, review, and destruction of safeguarding records.
- Support safe and effective safeguarding practices that prioritise athlete welfare and protection at all times.

By adopting this policy, IGA reaffirms its commitment to promoting a safe, transparent, and supportive sporting environment, where safeguarding and data protection are integral parts of organisational responsibility.

Purpose

The purpose of this policy is to ensure that safeguarding and welfare-related records held by the Independent Gymnastics Association (IGA) and its affiliated clubs are managed responsibly, securely, and in accordance with legal and safeguarding requirements in every jurisdiction in which IGA operates. This policy provides a structured framework to:

- Protect children and adults at risk by ensuring accurate and timely recording of safeguarding concerns, actions, and decisions.
- Support effective safeguarding practices by retaining records for as long as they may be needed to protect individuals, inform investigations, or respond to future concerns.
- Comply with legal and regulatory obligations regarding data protection, privacy, information sharing, and child protection across England & Wales, Scotland, Northern Ireland, the Republic of Ireland, and the Channel Islands.
- Uphold data protection principles, including confidentiality, lawful processing, security, and storage limitation.
- Clarify organisational responsibilities for handling, reviewing, sharing, and securely disposing of safeguarding information.
- Ensure transparency and consistency so that all clubs understand what records must be kept, why, for how long, and who can access them.
- Enable cooperation with statutory agencies, such as safeguarding partners, law enforcement, child-protection services, and regulators.

By defining the lawful, fair, and proportionate management of safeguarding information, this policy reinforces IGA's commitment to maintaining a safe, trusted, and compliant environment for every gymnast, volunteer, and workforce member.

Scope

This policy applies to the Independent Gymnastics Association (IGA) and to all affiliated member clubs, organisations, and personnel who handle safeguarding or welfare-related information. It sets out the required standards for recording, storing, sharing, retaining, reviewing, and securely disposing of such records.

Individuals Covered
This policy applies to:

- IGA Board members, senior leaders, and administrators
- Club owners, managers, and safeguarding leads
- Coaches and technical staff
- Welfare Officers and safeguarding personnel
- Volunteers, contractors, and any individual acting on behalf of IGA
- Third-party service providers who process safeguarding data on IGA's behalf

All individuals within scope must understand and comply with their responsibilities for managing safeguarding information appropriately.

Records and Information Covered
This policy applies to any information that is created, held, or processed in relation to safeguarding and welfare matters, including (but not limited to):

- Safeguarding concerns, referrals, and incident reports
- Child protection records and welfare case files
- Allegations or conduct concerns relating to staff or volunteers
- Notes and records from safeguarding meetings or strategy discussions
- Parental consents and information-sharing decisions
- Health or medical information relevant to gymnast protection
- DBS / vetting, qualifications, and safeguarding-training records
- Communications relating to safeguarding decisions (email, written, digital)

If a record contains or relates to safeguarding information, this policy applies, regardless of format.

Data Formats Covered
This policy covers safeguarding information in any form, including:

- Paper files
- Electronic records
- Secure digital platforms and cloud storage
- Messaging and communication platforms (email, SMS, internal systems)
- Audio, visual, or photographic media used for safeguarding purposes

Wherever information is recorded or stored, appropriate safeguards must be applied.

Geographic and Jurisdictional Scope
This policy must be followed in all jurisdictions in which IGA operates:

- England & Wales
- Scotland
- Northern Ireland
- Republic of Ireland
- Channel Islands (e.g. Jersey, Guernsey, Alderney)

Where local laws or guidance differ, the stricter requirement must always be applied, and clubs must ensure any local jurisdiction-specific obligations are met.

Activity Scope
This policy applies:

- At all IGA-sanctioned activities
- During training, camps, events, travel, and competitions
- To all safeguarding-related information created both inside and outside the gym environment

Legal & Regulatory Framework

This section summarises the principal laws, regulations, and statutory guidance that govern the handling, retention, sharing, and destruction of safeguarding and welfare-related data for IGA and affiliated clubs. It provides the legal foundation for the rest of the policy.

UK — Data Protection: UK GDPR & Data Protection Act 2018

- Within the UK jurisdictions (England & Wales, Scotland, Northern Ireland), the processing of personal data — including safeguarding, health or welfare data — is governed by the UK General Data Protection Regulation (UK GDPR) and domestic Data Protection Act 2018 (DPA 2018).
- These laws require that personal data be: processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and, where necessary, kept up to date; kept no longer than necessary (storage limitation); and processed in a secure manner.
- For particularly sensitive data — for example health data or safeguarding/child-protection information — the law recognises "special category data." Processing such data requires a valid lawful basis (under Article 6) and an additional condition under Article 9 / DPA 2018. In safeguarding contexts, the condition of "safeguarding of children and of individuals at risk" (under Schedule 1 of the DPA 2018) can apply, providing a lawful basis for processing or sharing without consent when necessary to protect individuals from harm.
- Importantly: data-protection law does not prohibit sharing safeguarding data when a child or individual is at risk — in fact, it provides a legal framework to enable appropriate, proportionate, and lawful sharing for safeguarding purposes.

Safeguarding / Child-Protection Legal & Statutory Framework (UK Nations)

- The safeguarding and child-protection system in the UK is devolved: each home nation (England, Wales, Scotland, Northern Ireland) has its own legislation and statutory guidance governing child welfare and protection.
- Organisations working with children — including sports clubs — have a duty of care to safeguard their welfare, prevent harm, and report concerns under the relevant national frameworks.
- For children's safeguarding, data-protection obligations and safeguarding duties must be balanced: protection of privacy is important, but when there is risk of harm, safeguarding obligations may override. The guidance from statutory safeguarding procedures affirms that correct information-sharing is often necessary to protect children.

Data Sharing for Safeguarding — Guidance & Principles

- The Information Commissioner's Office (ICO), the UK's data-protection regulator, explicitly states that data protection law does not prevent organisations from sharing information when required to safeguard a child — provided the sharing is lawful, fair, proportionate, and underpinned by a defined lawful basis.
- The ICO's "10-Step Guide to Sharing Information to Safeguard Children" sets out good practice for organisations handling safeguarding data: define the purpose, share only what is necessary, ensure secure systems, document decisions, and regularly review policies and procedures.
- In sport and youth-work contexts, obligations to safeguard children and young people supersede purely administrative concerns about data privacy — i.e. "if you have reason to believe a child is at risk, you must share what you need to." This principle applies equally to clubs, coaches, welfare officers, and administrators.

International / Non-UK Jurisdictions: Ireland, Channel Islands — Local Law & Complementarity

- Where IGA operates outside the UK — for example in the Republic of Ireland, and in Crown Dependencies such as the Channel Islands — clubs must also comply with local data-protection and safeguarding legislation in addition to UK-based standards.
- For example: in Ireland, safeguarding in sport is guided by national frameworks such as Children First Act 2015 and accompanying guidance for organisations working with children; national guidance emphasises creating a "safe and positive environment" for children's sport, child-centred safeguarding statements, and robust record-keeping.
- In any jurisdiction, where local law or statutory guidance sets a higher standard (for data protection, record-keeping, confidentiality, child-welfare, or information-sharing), those higher standards must take precedence.

Data Protection & Safeguarding: How They Interact

- The policy — and all its practices — must respect both data-protection and safeguarding obligations. This means clubs must:
  a. Use lawful bases for processing safeguarding data (e.g. vital interest / public interest / legitimate safeguarding need) rather than relying solely on consent in all cases.
  b. Apply data-protection principles (limitation, necessity, security, accuracy, confidentiality, storage limitation) when collecting and storing data.
  c. Enable information-sharing when needed for safeguarding — even where consent cannot be obtained — provided sharing is justified, proportionate, and documented.

d. Securely store data and restrict access on a "need-to-know" basis. Sensitive data (e.g. medical, child-welfare) must have enhanced protection and only be accessed by authorised persons.
e. Retain records only as long as reasonably needed, and have in place secure disposal or archiving processes. This must consider both safeguarding needs and data-protection storage limitation principles.

- In practice, this means that safeguarding-related data may need to be retained longer than ordinary data — especially where there is potential for future risk, historical investigation, or regulatory requirement — but retention must always be justified, documented, and subject to periodic review (see Retention Schedule section).

Regulatory & Governance Oversight

- As a data controller or data processor under UK law, IGA (and its clubs) may be subject to audit or enforcement by data-protection supervisory authorities (e.g. ICO in UK).
- Failure to process or share information appropriately (e.g. failing to share safeguarding concerns because of over-emphasis on privacy) can constitute a breach of safeguarding obligations and, in some cases, statutory duties.
- Therefore, this policy aims to ensure IGA's practices meet both data-protection and safeguarding standards — balancing individuals' privacy rights with the welfare and safety needs of gymnasts.

Data Protection Principles & Lawful Bases for Safeguarding Data

This section describes the fundamental data protection principles that must govern all processing of safeguarding, welfare, and related personal data — and outlines which lawful bases are appropriate when IGA and its member clubs collect, store, share, or dispose of such data.

Core Data Protection Principles

All processing of personal data under this policy must adhere to the key data-protection principles set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), namely that data must be:

- Processed lawfully, fairly, and transparently.
- Collected for specified, explicit, and legitimate purposes (purpose limitation).
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
- Accurate and, where necessary, kept up to date.
- Kept no longer than necessary for the purposes for which they are processed (storage limitation).
- Processed in a manner ensuring appropriate security (integrity and confidentiality) — protecting against unauthorised or unlawful processing, loss, destruction or damage.

In addition to these, given the context of safeguarding and working with minors, the processing must be designed with particular care and sensitivity. As described by the ICO — extra protections and considerations are needed when processing children's personal data.

Special Category Data and Sensitive Information

Many safeguarding and welfare records — health information, safeguarding concerns, child-protection data, medical or psychological notes — will amount to "special category data" under the UK GDPR.

Because of the sensitivity of such data:

- Processing must satisfy a valid legal basis under Article 6 of the UK GDPR and an additional condition under Article 9 / DPA 2018.
- Clubs must treat such data with enhanced confidentiality, apply strict access controls, and ensure security and necessity of processing.

Lawful Bases for Safeguarding Data Processing

Before any processing of personal data occurs, IGA / clubs must identify and document a lawful basis for that processing, as required by the UK GDPR.

For safeguarding and welfare-related data processing, the most relevant lawful bases include:

Lawful Basis	When It Applies / Why It Is Suitable
Legal Obligation (Article 6(1)(c))	When processing is necessary to comply with statutory safeguarding or child-protection duties, or other legal requirements.
Public Task / Official Function (Article 6(1)(e))	For processing required to carry out IGA's functions in the public interest — e.g., protecting the welfare of children and vulnerable individuals
Vital Interests (Article 6(1)(d))	In emergency or life-threatening situations where processing is necessary to protect the life of a data subject. (Although this basis has limited use for
Consent (Article 6(1)(a)) *(and where special category data, explicit consent under Article 9)*	When it is appropriate and realistic to obtain informed, freely given consent — for example for health-related data or parental consent for minors

Important considerations:

- Consent is not always appropriate, especially in safeguarding contexts — because individuals (or children) may not be in a position to give valid informed consent, or because safeguarding obligations may require data sharing regardless of consent. The ICO notes that data protection law does not prevent sharing information when required to safeguard a child.
- For processing special-category data (e.g., health, medical, safeguarding history), an Article 9 / DPA 2018 condition must be satisfied in addition to Article 6 — commonly "safeguarding of children and individuals at risk."
- For each processing activity, the chosen lawful basis should be documented and linked to a clearly defined purpose. This is good practice and helps meet transparency and accountability obligations.

Special Considerations for Children's Data

Because IGA works extensively with minors, additional care must be taken:

- Children's data is particularly sensitive; extra protection, transparency, and fairness must be embedded from the outset.
- When relying on consent for processing a child's data, you must ensure the child (and/or parent/guardian) genuinely understands what they are consenting to — and that consent is freely given.
- In many safeguarding contexts, consent is not relied upon: instead, public interest / legal obligation / vital interest / public task bases may be more appropriate.
- Organisations should design their data-processing and information-sharing arrangements from the outset with children's rights, vulnerability and best interests in mind.

Data Minimisation, Necessity & Proportionality

- Only the minimum personal data necessary for safeguarding purposes should be collected and processed.
- Organisations should avoid "blanket" data collection simply "in case it might be needed" — every piece of personal data must have a clear, documented purpose.
- Any further data sharing must be evaluated case-by-case: ensure it is proportionate, necessary, and appropriate considering the sensitivities of safeguarding data.
- Special-category and safeguarding data should be shared only with those who need to know (e.g., welfare officers, medical professionals, statutory safeguarding agencies).

This aligns with the ICO's guidance that data-protection law is not a barrier to safeguarding — but must be applied properly to respect privacy and rights.

Documentation, Transparency & Accountability

IGA and its clubs must:

- Maintain a record (data-map or data-register) of all processing activities concerning safeguarding / welfare data — what data is held, why, lawful basis, retention period, who can access, when it will be destroyed or reviewed.
- Provide transparency to data subjects (or, for minors, to parents/guardians) — explaining what data is collected, the purpose, who it may be shared with, their rights under data protection law.
- Review and document lawful basis and necessity each time new data is collected, shared, or retained — especially when processing special category data.
- Be able to justify retention (or deletion) decisions using documented criteria.
- Perform periodic audits / reviews to ensure compliance with data-protection and safeguarding standards.

Interaction with Safeguarding Obligations

Data protection and safeguarding are complementary, not contradictory. Under the guidance of the ICO and statutory safeguarding protocols:

- You must share relevant personal data where required to protect a child or vulnerable person — data protection law does not prevent this.

- Safeguarding must always take precedence: if there is risk of harm, sharing information to protect the individual is a lawful and necessary act.
- At the same time, sharing should be proportionate and limited to what is strictly necessary, following the principles above (minimisation, confidentiality, necessity).

Data Protection Principles & Lawful Bases for Safeguarding Data

All safeguarding and welfare-related data processed by the Independent Gymnastics Association (IGA) and affiliated clubs must comply with the data protection legislation applicable in their jurisdiction. For the UK, this includes the UK GDPR and Data Protection Act 2018, which set out the core expectations for lawful and responsible data handling.

Core Data Protection Principles
IGA and its clubs must ensure that all safeguarding data is:

- Lawfully, fairly and transparently processed
- Collected only for specific and legitimate safeguarding purposes
- Relevant and limited to what is necessary for protection and welfare
- Accurate and updated where needed
- Retained only as long as necessary, with regular review
- Kept secure and confidential, with controlled access and protection against loss or misuse

These principles are legal requirements placed on any organisation handling personal data.

Special Category Data
Safeguarding and welfare records typically include special category data (e.g., health, mental well-being, risk disclosures, incident reports). Such data requires:

- A lawful basis under Article 6 UK GDPR
- An additional condition under Article 9 for processing special category data

Because it carries a risk of significant harm if mishandled, enhanced confidentiality and access controls must always be applied.

Lawful Bases Relevant to Safeguarding
IGA and clubs must identify and document a lawful basis for each processing activity. Common lawful bases for safeguarding data include:

Lawful Basis	When Used
Legal Obligation	Where a safeguarding law requires action to protect a child/vulnerable person.
Public Task	When carrying out safeguarding functions in the public interest (e.g., duty of care in children's sport).
Vital Interests	In emergencies where processing is required to prevent serious harm or protect life.
Consent	Only where freely given, informed, and realistic in context — **not appropriate for most safeguarding**.

The ICO confirms that data protection law does not prevent information being shared if a child is at risk of harm, provided sharing is necessary and proportionate.

Children's Data — Heightened Duties
As IGA primarily works with children and young people:

- Their data must be handled with enhanced protection and transparency
- Consent must only be used if the child (and parent/guardian) can meaningfully understand and freely choose
- Where risk of harm is present, lawful sharing proceeds even without consent in line with safeguarding duties
- The best interests of the child must always guide decisions

Children's safeguarding data has zero tolerance for unauthorised access or misuse.

Necessity, Minimisation & Proportionality
Only the minimum data necessary to protect a child or vulnerable person may be collected or shared. IGA and clubs must not retain or process safeguarding data "just in case"; every item must have:

- A clear purpose
- A documented lawful basis
- A defined retention schedule

Decisions must be proportionate to both risk and sensitivity.

Accountability & Documentation
Clubs must:

- Maintain a record of processing activities for safeguarding data
- Justify lawful basis and retention decisions
- Restrict access to those with a legitimate safeguarding need
- Audit compliance regularly
- Ensure secure systems for both physical and digital records

These expectations align with regulator guidance for organisations handling children's data and safeguarding information.

Safeguarding Takes Precedence When Necessary
Where there is immediate risk of harm, safeguarding duties override normal restrictions on sharing:
If there is reason to believe a child may be at risk, information must be shared appropriately — promptly, lawfully, and securely — to protect them.

Safeguarding and data protection are complementary, not conflicting.

Types of Records Covered

This policy applies to all records — in any format — that relate to safeguarding, welfare, health, and protection of gymnasts, staff or other individuals associated with IGA.

Child Protection & Safeguarding Case Files
- Reports of safeguarding concerns (past or current)
- Allegations against staff, coaches, volunteers or third parties
- Reports made by athletes, third-parties or via disclosure
- Records of investigations, actions taken, outcomes, safeguarding plans, follow-up reviews

Welfare, Health, Medical & Psychological Records
- Medical assessments, diagnoses, referrals, treatment plans relevant to gymnast welfare
- Nutrition, dietician or physiotherapy records — where related to safeguarding, health, eating disorders or energy-availability concerns
- Records of weighing, growth monitoring, body composition assessments, health-check forms
- Mental health or well-being assessments, counselling or therapy notes (if relevant to safeguarding)

Consent, Permissions & Information-Sharing Documents
- Consent forms for medical treatment, weighing, nutritional plans, data-sharing
- Parent/guardian consent forms for minors
- Information-sharing agreements (e.g. between IGA, club, medical professionals, external agencies)
- Data-sharing logs — who data was shared with, when and why

Training, Vetting & Compliance Records
- Records of staff/coach/volunteer safeguarding training (dates, content, completion)
- Vetting or background-check records (e.g. disclosures, qualifications, suitability checks)
- Compliance audit records, policy acceptance declarations, safeguarding briefings

Administrative & Communication Records
- Correspondence (email, letters, meeting minutes) relating to welfare or safeguarding concerns
- Meeting records (safeguarding meetings, welfare reviews)
- Notes from welfare-officer meetings, debriefings or risk assessments
- Logs of support or referrals made (medical, psychological, external agencies)

Incident & Event Records

- Reports of injuries, health crises, accidents — especially those relevant to nutrition, growth or health risks
- Records of any disciplinary or welfare-related incidents linked to dieting, weight pressure, body-image concerns, or related complaints
- Records of interventions, monitoring, and follow-up actions

Historical / Archived Files

- Closed safeguarding or welfare cases (with summary, outcome, date of closure)
- Archived documentation of previous assessments, interventions or safeguarding plans
- Archived consent and data-sharing history

Data-Sharing & External Agency Records

- Records of data shared with external agencies (child-protection authorities, medical professionals, regulators), including what was shared, when, and legal basis
- Agreements with third-party service providers or contractors handling safeguarding data on behalf of IGA or clubs

Formats Covered

This policy applies to safeguarding and welfare records in all forms, including:

- Paper-based records (files, signed forms, printed reports)
- Electronic or digital files (databases, spreadsheets, PDFs)
- Emails, messages, correspondence (digital or paper)
- Audio or video recordings (if used for safeguarding, consent, or welfare monitoring)
- Notes — meeting minutes, supervision notes, verbal disclosure records

Boundary of Coverage

Any record that includes or relates to safeguarding, welfare, health, consent or protection falls under this policy.

If uncertain, clubs should err on the side of inclusion — treat the record as covered to ensure protection and compliance.

Retention Principles & Standard Periods

This section establishes the principles that guide how long safeguarding, welfare, and related data should be retained, and provides recommended standard retention periods (or retention rules) for key types of records.

Overarching Retention Principles

When determining how long to keep records, IGA and its clubs must observe the following principles:

- Necessity & Purpose: Records should be retained only as long as they are needed for safeguarding, welfare, legal or regulatory purposes. Once the purpose no longer applies — or the legal requirement lapses — records should be securely destroyed.

- **Security and Confidentiality:** Throughout their lifecycle (storage, retention, destruction), safeguarding records must be stored securely, with access limited to authorised personnel only.
- **Flexibility for Ongoing Risk or Legal Requirements:** Records must be retained longer if needed to manage ongoing safeguarding concerns, potential investigations, legal claims, historic abuse disclosure or other regulatory obligations.
- **Regular Review:** Retention schedules should be reviewed periodically (e.g., annually) to confirm that retained data is still necessary, and to identify records eligible for secure destruction.

These principles align with widely accepted guidance for safeguarding-record retention and data-protection obligations.

Recommended Retention Periods / Retention Rules
Given the variety of record types covered under this policy (see Section 6), the following table outlines recommended minimum retention periods or retention rules for key categories. Because there is no single "statutory" retention period applicable to all safeguarding data, these recommendations follow best-practice guidance from organisations such as NSPCC, the Child Protection in Sport Unit (CPSU), and education-sector retention guidelines in the UK.

Record Type / Description	Recommended Retention Period / Rule
Child protection / safeguarding case files (concerns, disclosures, investigations, outcome reports)	Until child's 25th birthday (or 25 years beyond date of birth) — or equivalent of "child + 7 years after reaching adulthood" where practical. If record includes child-sexual-abuse allegations, or serious harm concerns, consider extended retention (see row below). (GOV.UK)
Records related to child-sexual-abuse allegations or serious harm	Retain for extended period — for example until child's 75th birthday, or as required by statutory inquiries or local authority safeguarding guidance. (GOV.UK)
Records of allegations against staff/volunteers (substantiated or unsubstantiated), vetting/DBS checks, risk assessments	Until the staff or volunteer reaches retirement age (or at least 10 years after allegation, whichever is longer) — consistent with established safeguarding-in-sport best practice guidance. (cambslearntogether.co.uk)
Welfare / health / medical / diet / nutrition / psychological records (where related to safeguarding, vulnerability, or health risk)	Retain for a reasonable period after the last relevant contact — e.g., 7 years after last intervention or closure of case — unless longer retention is justified (e.g., ongoing risk). This aligns with general guidance used by voluntary/community organisations. (ICMEC)

Consent forms and information-sharing permissions (for minors)	Keep for the duration of the case plus a retention period consistent with the associated safeguarding files (i.e., until at least
Training, vetting & compliance records (staff safeguarding training, safe-recruitment checks, compliance audits)	Retain for a minimum of 6 years after role ends (or last relevant activity), or longer if required for liability, regulatory or
Administrative, communication, meeting-minute records related to safeguarding / welfare	Retain a minimum of 7 years after last entry (or longer if part of a safeguarding case with extended retention rule) — to balance
Records of data-sharing with external agencies (child protection authorities, medical professionals, regulators)	Retain according to the longest retention rule applicable (e.g. safeguarding case file that prompted the sharing — see above).
Archived / closed case files (safeguarding, welfare, historic concerns)	Keep in secure, separate archive, until end of retention period indicated above for that record type. Periodic review recommended to

IApplication of the "Longer Retention Where Risk or Legal Requirement" Rule

GA and clubs must recognise that:

- Where there is ongoing risk, delayed disclosure (e.g., historic abuse), or potential for future legal action, retention periods should be extended accordingly.
- Retention must never be mechanistic — decisions to destroy must involve a review of risk, legal context, and organisational history.
- Destruction of records must be documented, with date of destruction, who authorised it, and confirmation that this does not breach any known or potential legal or safeguarding obligation.

This approach reflects the caution urged in guidance from the NSPCC and CPSU: that organisations should "assess how long you need to keep records for" and "have a plan for how and when the records will be destroyed."

Secure Disposal & Record Destruction Standards

When the retention period expires — or the organisation determines the data is no longer needed — records must be destroyed securely, in such a way that data cannot be reconstructed or retrieved. For example:

- Paper records: shredding or incineration
- Electronic records: secure deletion, ensuring removal from backups, multiple overwrites where required
- Records on third-party storage services: ensure provider compliance and confirm secure erase

Destruction must be logged (when, what, by whom) to support audit, compliance, and accountability.

Periodic Review and Audit of Retention Policy
IGA will require all affiliated clubs to:

- Undertake annual reviews of their safeguarding data holdings, checking what records remain, why, and when they are due for destruction
- Use a master retention schedule (or log) to track files, retention dates, and destruction plans
- Report audits or any deviations or holding of records beyond retention to the central IGA Safeguarding / Data-Protection Lead

This ensures the policy remains live, accountable, and compliant with both safeguarding and data-protection expectations.

Jurisdiction-Specific Retention Considerations

IGA operates across multiple jurisdictions — each with its own data-protection regimes and safeguarding/child-protection contexts — this policy must be applied with sensitivity to local legal and regulatory obligations. Where local law or guidance sets stricter requirements than the baseline policy, those stronger requirements must prevail.

England & Wales, Scotland & Northern Ireland

- In UK jurisdictions, guidance from organisations such as NSPCC / Child Protection in Sport Unit (CPSU) recommends that safeguarding and child-protection files are retained until the subject's 25th birthday (i.e. until 7 years after majority), or longer where risk or serious harm (e.g. sexual abuse) is involved.
- Education-sector guidance in the UK also reflects the same baseline: child protection files should be retained until the young person's 25th birthday.
- For records related to allegations against staff or volunteers (substantiated or not), many organisations keep records for the duration of the person's working life (or until minimum specified periods) to allow for responses to future complaints or regulatory reviews.
- Where cases involve serious harm, abuse, or potential long-term risk, UK guidance recommends extending retention — potentially indefinitely.

Implication for IGA in UK regions: Use the standard retention rules as a minimum — but for any safeguarding concerns, especially those involving abuse or serious risk, apply extended or indefinite retention. Document decisions and reviews carefully.

Channel Islands (e.g. Jersey, Guernsey / Bailiwick of Guernsey)

- In Jersey, under the Data Protection (Jersey) Law 2018 — like most data-protection laws — there is no statutory fixed retention period. Instead, the "storage limitation" principle applies: data should be kept only as long as necessary for the purpose for which it was collected.
- Similarly, in Guernsey (under the Data Protection (Bailiwick of Guernsey) Law 2017), there is no fixed retention timetable; organisations must document their processing activities, purposes, retention rationale, and disposal plans.

- For public-authorities / social-care / child-welfare services in Jersey, there exist retention-schedule guidance for "Children's Social Care" records — including criteria for secure disposal or transfer to archive when appropriate.
- Local guidance emphasises that retention decisions should be justified by purpose, risk, and ongoing safeguarding needs — not arbitrary fixed periods.

Implication for IGA in the Channel Islands: Adopt a retention schedule based on necessity, risk, and safeguarding purpose. Document and justify retention decisions; review periodically. For serious safeguarding concerns (e.g. abuse, threats), treat as long-term records even if no statutory timeframe exists.

Republic of Ireland

- While this policy covers Irish operations, local data-protection and child-safeguarding legislation does not always prescribe uniform retention periods for safeguarding records in a sporting context.
- General data-protection principles (as per GDPR) apply — meaning records must be retained only for as long as necessary and deleted when no longer justified.
- Best practice when working with children includes retention until at least the child reaches adulthood + a reasonable number of years, especially for historic files involving risk or harm. International and European best-practice guidance for child-safeguarding records supports long-term retention where there is possibility of future disclosure or investigation.

Implication for IGA in Ireland: Use the standard retention schedule (child + 7 years / 25th birthday) as a minimum. For serious or risk-related safeguarding records, apply extended / long-term retention, while documenting purpose and ensuring confidentiality and security.

Cross-Jurisdiction Principles

Because IGA operates internationally across multiple jurisdictions:

- The most protective rule among applicable jurisdictions should be applied for any given record — whether that is a fixed retention period (e.g. UK 25-year guideline) or a justification-based retention (Channel Islands).
- For serious incidents — especially those involving abuse or risk of harm — retention should default to long-term or indefinite, regardless of local statutory minimums, to allow for future safeguarding concerns, possible disclosure, or legal/regulatory review.
- Clubs must maintain a record of retention decisions, including rationale, review dates, and disposal plans. This documentation is essential for compliance with data-protection laws that emphasise transparency, accountability, and necessity.
- Periodic review (e.g. every 2–3 years) of all retained safeguarding data is required. Clubs should assess whether there remains a legitimate safeguarding or legal need to hold each file; if not, secure disposal should be carried out.

Special Considerations and Exceptions

- Historic abuse disclosures / late reporting — given that abuse may be disclosed many years after events, safeguarding data (even if historical) should be retained long-term.

- Allegations against staff/volunteers — even if unsubstantiated, records should be retained for extended periods (staff career duration or longer), to allow reference in case of future complaints or investigations.
- Ongoing investigations or legal proceedings — all relevant records must be retained until final closure, and potentially archived beyond closure if legally or ethically justified.

Storage, Security & Access Controls

Given the sensitive nature of safeguarding, welfare, and health-related records, this section defines mandatory standards for storage, security, access, and handling of such data — whether held on paper or electronically.

Core Principles

- Confidentiality & Integrity: All safeguarding and welfare data must be treated as highly sensitive. That means strict measures to prevent unauthorised access, modification, or disclosure.
- Access on a 'Need-to-Know' Basis: Only individuals who require access for legitimate safeguarding, welfare or regulatory reasons may view or handle files. This should be defined and documented.
- Secure Storage: Both physical and electronic records must be stored in a secure environment, with appropriate protection against loss, theft, damage, or unauthorised access.
- Auditability & Accountability: Access and modifications to records must be logged; clubs must maintain an audit trail showing who accessed what, when, and for what purpose.
- Data Separation and Segregation: Safeguarding data must be segregated from general administrative records; sensitive data (e.g. health or child welfare) must not be mixed with routine club documents.
- Resilience & Backup: Digital systems should include secure backups to protect against data loss (e.g. due to hardware failure, cyber-attack, accidental deletion), but backups must themselves be subject to the same access and security controls.

Physical Records Storage (Paper Files)

For paper-based safeguarding and welfare records:

- Records must be stored in locked, access-controlled cabinets or rooms when not in use.
- Access keys or codes must be limited to designated safeguarding staff (e.g. Welfare Officer, senior safeguarding lead), and a register maintained of who holds keys/codes.
- Working copies may be taken out only when necessary, and must be signed out and signed back in. Temporary records must never be left unattended or accessible to unauthorised persons.
- Disposal of paper records must follow secure destruction procedures (see Retention / Disposal section): shredding, incineration, or another irreversible method; disposal must be logged.

Electronic Records Storage & Digital Security

For safeguarding data stored electronically:

- Data must be held on secure servers or trusted cloud services with robust security: encryption (at rest and in transit), strong authentication, firewalls, and up-to-date security patches.
- Where cloud or external hosting services are used, clubs must verify the data processor's compliance with relevant data-protection laws (e.g. UK GDPR, local law in Channel Islands or Ireland).

- Access control must be enforced via role-based permissions: only authorised staff (e.g. Welfare Officer, Data Protection Officer, senior management) may access safeguarding files.
- Multi-factor authentication (MFA) is strongly recommended for accounts with access to safeguarding data.
- Automatic logging must record: who accessed the data, when, what was viewed or modified, and why. Logs must be retained for a defined period to support audits.
- Regular backups must be made; backups must be encrypted and stored securely; backup systems must be subject to the same access controls.

Data Transmission & Sharing Security
When safeguarding or welfare data is transferred (e.g. sharing with external agencies, medical professionals, or across club branches):

- Use secure transmission methods only — encrypted email or secure file-transfer protocols. Never unencrypted email for personal or sensitive data.
- Attach a data-sharing consent and purpose statement to clearly indicate why the data is being shared, who will receive it, and how it must be treated.
- Maintain a data-sharing log documenting: what was shared, to whom, when, purpose, and lawful basis.
- Limit data sharing to the minimum necessary for the intended safeguarding function.

Access, Roles & Responsibility Management
Clubs must define and document roles and responsibilities for data access and management:

- Identify which roles (e.g. Welfare Officer, Data Protection Officer, Safeguarding Lead, Senior Management) are authorised to access which categories of data.
- Maintain an access register tracking authorised persons; update immediately whenever roles change or people leave.
- Provide training for any staff who may access safeguarding data — including data-protection awareness, confidentiality obligations, handling protocols, and security procedures.
- Ensure separation of duties where possible — e.g. the person approving access should not be the same as the person requesting it, and the person destroying data should not be the same as those who created it.

Incident Response & Breach Management
In the event of any actual or suspected data breach (loss, theft, unauthorised access, accidental disclosure):

1. The club must invoke its data-breach / safeguarding-incident procedures without delay.
2. The incident must be documented: what happened, when, who was affected, data involved, and likely impact.
3. Notify the central IGA safeguarding / data-protection lead immediately.
4. Notify external supervisory authorities as required by law (e.g. national data-protection regulator) — especially if personal or special-category data may have been compromised.
5. Review and, if needed, suspend access while assessing what happened. Implement corrective actions — e.g. changing access credentials, increasing security, re-training staff.
6. Inform affected parties, where appropriate, with transparency.

Breach response procedures must be tested and known to all staff with access to safeguarding data.

Data Protection & Confidentiality Culture

- To embed a culture of confidentiality and respect for privacy:
- All staff, volunteers and contractors should sign a confidentiality agreement upon induction, acknowledging their responsibilities under this policy and under relevant data-protection and safeguarding law.
- Ongoing training should reinforce data-protection principles, secure handling, and safeguarding confidentiality.
- Clubs should conduct periodic audits (e.g. annually) to verify access logs, storage security, destruction records, and compliance with this section.
- Reviews should include testing of digital security (e.g. penetration testing, verifying encryption), audits of physical storage, and checks of staff access permissions.

Local Jurisdiction & Data-Protection Compliance

Because IGA operates across multiple jurisdictions (UK, Republic of Ireland, Channel Islands):

- Storage and data-handling practices must comply with the strictest applicable standard among relevant laws (for example, including local data protection laws in Jersey, Guernsey, or Ireland).
- External hosting providers (cloud, servers) must be vetted for compliance under the relevant local data-protection regimes.
- Data access and sharing with agencies in different jurisdictions must observe cross-border data-transfer safeguards — including encryption, secure transfer protocols, and adherence to local data-protection requirements.

Data Sharing, Multi-Agency Working & Cross-Border Transfers

When Sharing Information Is Appropriate

IGA and its affiliated clubs may share safeguarding-, welfare- or health-related data when:

- There is a reasonable belief of risk or harm to a gymnast (child or adult at risk) that requires multi-agency intervention.
- There is a need to consult, refer, or cooperate with external services — such as social care, medical professionals, safeguarding partners, law enforcement, or regulatory authorities.
- Sharing is necessary to fulfil statutory safeguarding obligations, or to protect the physical or mental well-being of a child or vulnerable individual.
- There is a compelling welfare need — even where consent cannot be obtained or where seeking consent would delay or jeopardise protection.

Guiding Standards: Following ICO's 10-Step Guide

When sharing safeguarding data, IGA and clubs must follow the principles set out in the ICO's "A 10 Step Guide to Sharing Information to Safeguard Children":
Key steps include:

1. Be clear about why data is being shared (the safeguarding objective)
2. Share only information necessary for that objective (data minimisation)
3. Use secure and appropriate mechanisms for sharing
4. Document decisions, the lawful basis for sharing, and parties involved
5. Ensure transparency and respect for data-subject rights, balanced with safeguarding needs
6. Where sharing is regular or ongoing, establish formal data-sharing agreements between agencies/organisations

Lawful Bases for Sharing (including Sensitive / Special-Category Data)

- Sharing may rely on legal bases under data-protection law such as "public task / official duty", "vital interests"or "legal obligation / substantial public interest" rather than consent — especially relevant when dealing with safeguarding, child-protection or medical data.
- For sensitive or special-category data (health, welfare, abuse history), sharing is permissible under conditions relating to safeguarding of children or individuals at risk, even where consent is not given, if obtaining consent is not feasible or could prejudice protection.
- Consent remains important where appropriate and feasible, but should not be treated as the only lawful basis when safeguarding is at stake.

Multi-Agency Working & Information Sharing Agreements

Where clubs routinely interact with external organisations (e.g. social services, medical professionals, child-protection agencies), the following must be in place:

- A formal data sharing agreement or protocol that sets out:
  - What data may be shared
  - Who can receive it
  - For what purpose
  - Obligations for confidentiality and security
  - Review and audit procedures

- Clear procedures for recording data-sharing events, including: what was shared, with whom, when, and why.
- Periodic review of these agreements and procedures, especially if circumstances change (e.g. new local agencies, cross-border issues, updated legislation).

Cross-Border Data Transfers & Jurisdiction Considerations

Given that IGA operates across multiple jurisdictions (e.g. UK nations, Republic of Ireland, Channel Islands), special care must be taken when safeguarding data crosses borders, or is shared with agencies operating under a different legal regime:

- Only transfer data if there is a clear safeguarding justification, and ensure the transfer is lawful under relevant data-protection legislation for both the sending and receiving jurisdiction.
- Use secure, encrypted data-transfer methods when sharing electronically.
- Where possible, enter inter-jurisdictional data-sharing agreements or memoranda of understanding (MoUs)clarifying legal bases, data handling expectations, and responsibilities.
- Maintain records of cross-border transfers, including legal basis, purpose, destination, and parties involved.

Emergency Situations & Urgent Data Sharing

- In emergency or life-threat scenarios where a child or individual is at risk of serious harm, data may be shared immediately and without delay, even if consent cannot be obtained — provided sharing is necessary and proportionate.
- Such cases must be documented carefully: who made the decision, when, what was shared, and why — and followed up with appropriate reporting and safeguarding procedures.

Documenting and Auditing Data Sharing
To ensure accountability and compliance:

- Every data-sharing event must be logged (what, why, when, with whom, lawful basis)
- Records of data-sharing decisions must be retained as part of the safeguarding record-keeping system
- Periodic audits should be conducted to ensure data-sharing is lawful, necessary, and proportionate — especially when data is regularly shared with external agencies or across borders

Transparency, Privacy Notices & Data-Subject Rights

- Individuals (or their parent/guardian, for minors) should be informed, via privacy notice or other means, that their data may be shared for safeguarding purposes — and under which circumstances.
- However, in safeguarding cases where sharing without consent is justified, transparency may be limited where informing the subject could jeopardise safety — but decision-making must be documented and reviewed.
- Where lawful, data-subjects retain rights under data-protection law (access, rectification, etc.); but safeguarding obligations and statutory conditions may override or limit those rights — as per relevant legislation.

Data Subject Rights & Requests

Under data-protection legislation (e.g. UK GDPR / Data Protection Act 2018, and equivalent law in other jurisdictions covered by IGA), individuals whose personal data is processed have specific rights. This section explains how those rights apply to safeguarding, welfare, and child-protection data held by IGA or its affiliated clubs — and any limits or adaptations needed given safeguarding duties.

Because safeguarding data often involves special-category data, and may concern minors or individuals at risk, exercising rights must always balance privacy and data-subject rights with child or vulnerable-person protection, statutory obligations, and confidentiality requirements.

Rights of Data Subjects Covered by This Policy
IGA recognises that data subjects have — where applicable under the law — the following rights:

- Right of access (to see what personal data is held)
- Right to rectification (correct inaccurate or incomplete personal data)
- Right to restriction of processing (in certain circumstances)
- Right to erasure / deletion ("right to be forgotten")
- Right to portability (where applicable), in certain contexts
- Right to object to processing (in certain circumstances)
- Rights relating to automated decision-making or profiling (rare in safeguarding context)

These rights apply in principle to all personal data processed — including safeguarding and welfare-related information — but may be subject to limitations given the nature of such data.

Managing Data Subject Requests: Procedures & Considerations

When a data subject (or for minors, their parent/guardian) submits a request under their data-protection rights, the following procedures apply:

1. Receipt of Request
   - All requests must be directed to the club's Data Protection Officer, Safeguarding Lead, or other designated person as specified by local club policy.
   - The request should be acknowledged promptly (e.g. within statutory timeframe — typically 1 month under GDPR / relevant law), and the requester should be informed if further verification or clarification is needed.
2. Verification and Identity Checks
   - Before providing any personal or safeguarding data, the club must verify the identity of the requestor — especially for sensitive welfare or child-protection records — to avoid unintended disclosures.
   - For minors, checks should ensure that consent or legal responsibility resides with the person requesting data (e.g. parent/guardian), while safeguarding the child's rights and dignity.
3. Assessment of Request vs Safeguarding Obligations
   - The club must assess whether fulfilling the request:
     - Is compatible with safeguarding duties, confidentiality, and third-party privacy (e.g. other children, staff, witnesses)
     - Might interfere with ongoing safeguarding investigations, legal proceedings, or risk future harm
   - If releasing data would pose risk to a child or third party, the club may lawfully refuse, redact, or limit the information provided — in line with data-protection law and statutory safeguarding guidance
4. Decision and Response
   - The club must respond in writing, within statutory deadlines, either providing the requested data / information, or explaining valid reasons for refusal or partial redaction — referencing the lawful basis and/or safeguarding duty that grounds refusal
   - When appropriate, the requester should be offered a summary of the relevant information (rather than full disclosure), to protect privacy of others or safeguarding confidentiality
5. Logging and Documentation
   - All requests, decisions, data provided, redactions or refusals must be logged
   - Details should include date of request, identity verified, data released (or withheld), rationale for decisions, and any follow-up actions
6. Appeals / Complaints
   - Data subjects (or guardians) must be informed of their right to appeal the decision internally (e.g. to a senior safeguarding officer or IGA central lead)
   - They also retain right to complain to the relevant data-protection supervisory authority (e.g. ICO in UK, relevant authority in Channel Islands or Ireland) if they believe their rights have been breached

Limits on Rights — Safeguarding Exceptions
Because safeguarding data often involves sensitive and potentially harmful information, certain rights may be limited or refused, including:

- Right to erasure / deletion — not guaranteed: safeguarding records often need to be retained for long-term risk management, legal obligations, historic disclosure possibilities, or statutory record-keeping requirements.
- Right of access — may be limited or redacted when full disclosure could endanger a child, third party, or compromise confidentiality of other individuals.
- Right to portability — rarely applicable for safeguarding data, due to complexity, sensitivity, and need for secure transfer; clubs may refuse when sharing could compromise safety or confidentiality.
- Right to object / restrict processing — may not apply where processing is required for safeguarding, child-protection, or legal obligations that override individual consent or choice.

All such decisions must be carefully documented, citing the relevant legal or safeguarding justification.

Transparency & Information to Data Subjects
IGA and clubs must provide clear privacy information to data subjects (or their guardians) at point of data collection, or as soon as practicable, explaining:

- What data is being collected and why
- Who may access or receive data (e.g. welfare officers, statutory agencies)
- How long data will be retained (or the criteria for retention)
- The rights of data subjects, and how to make a request
- Any limits to those rights in safeguarding contexts (e.g. potential redaction, refusal)

Where immediate full transparency might not be safe (e.g. in active safeguarding cases), clubs should issue a general data-protection notice explaining that data may be shared or retained as needed for safeguarding, alongside contact details for the Safeguarding / Data Protection Lead.

Data Subject Rights in Cross-Jurisdiction Contexts
Because IGA operates in various jurisdictions (UK nations, Republic of Ireland, Channel Islands):

- Data subject rights under local law must be respected — including any regional variations in statutory timeframes, scope of rights, or supervisory authority.
- Clubs must ensure that response procedures align with the most protective local standards.
- Supervisory authority contact details (e.g. regulatory bodies for data protection in each jurisdiction) must be maintained and provided as part of privacy information.

Disposal & Destruction of Records

IGA and all affiliated clubs must handle disposal of safeguarding, welfare, and sensitive personal data with the same care and privacy protections as during storage and processing. This section describes how and when records should be securely destroyed — and the documentation required to ensure accountability.

Principles for Disposal

- Data minimisation and necessity — once data is no longer required for safeguarding, welfare, legal, or regulatory purposes, it should be securely destroyed.
- Secure and irreversible destruction — disposal must render the data irrecoverable, whether physical or digital.
- Documentation and auditability — every disposal action must be logged: what was destroyed, when, by whom, and under which authority/retention-rule.
- Respect for potential future needs — disposal should not occur if there is any reasonable possibility of future need (e.g. historic disclosures, investigations, legal claims, audits). In those cases, data should be archived rather than destroyed.
- Consistency across jurisdictions — disposal must respect local data protection and safeguarding laws; where law requires longer retention, disposal must not proceed until that requirement is met.

When Records Should Be Considered for Disposal

Records may be considered for disposal when:

- The retention period specified for their record type has expired (see Retention Schedule section) and no ongoing risk or legal reason exists for further retention.
- The case is closed, there are no pending investigations or appeals, and no expectation of future use (e.g. no risk of re-opening).
- Consent-based records where the data subject has requested erasure, and there is no overriding safeguarding, legal or regulatory requirement to retain.
- Administrative, duplicate, or outdated records that no longer serve any safeguarding, compliance, or audit purpose.

Before disposal, a review must be conducted to confirm that no other safeguarding, legal, regulatory, or archival requirement applies.

Methods of Secure Disposal

Physical / Paper Records

- Paper records must be destroyed in a manner that ensures irreversible destruction — e.g.:
  - Cross-cut shredding (preferred)
  - Industrial shredding or incineration (where appropriate)
- Disposal of sensitive documents must not be placed in general waste or recycling.
- All disposal must take place in a secure environment — ideally overseen or conducted by authorised safeguarding or data-protection staff.
- A destruction log must be completed detailing the record reference, date, method, and the person authorising and performing destruction.

Electronic Records (Digital / Cloud / Storage Systems)

- Digital files must be securely deleted using appropriate deletion tools or processes that ensure data cannot be restored (not merely "move to trash").
- For cloud or third-party hosted storage: ensure the provider's deletion is comprehensive — including backups, archived versions, and any replicated data.
- Overwriting, degaussing or secure erase may be required depending on storage media and sensitivity.
- Log the deletion in a digital destruction register, noting the file(s), date, method, and authorisation.

Backup Media

- Backup media (physical or cloud-based) must also be considered; when records are scheduled for destruction, any copies or backups should also be securely deleted or destroyed, if not required for legitimate reason (e.g. legal, archival, regulatory).
- Where deletion of backups is not immediately practical, a flagging or suppression mechanism should be used — ensuring data is no longer accessible or processed — until final disposal is possible.

Documentation & Audit Trail

For each disposal event (physical or digital), clubs must maintain a Destruction Log containing at least:

- Reference to the record(s) destroyed (file name / ID / category / date range)
- Date and time of destruction
- Method of destruction (shredding, secure delete, etc.)
- Name and role of person authorising disposal
- Name and role of person performing disposal
- Confirmation that no active investigations, litigation, or future obligations exist
- Where relevant, confirmation that backups and duplicates have also been destroyed (or suppressed)

Logs must be retained for a minimum of 6 years after destruction, or longer if required by local law — so there is an audit trail proving compliance with the retention and destruction policy.

Suspension of Destruction Where Risk or Investigation Exists

Records must never be destroyed if:

- There is an ongoing safeguarding investigation, complaint, or legal proceeding
- There is a credible risk of future disclosure (e.g. historic abuse, late reporting)
- The data relates to serious harm, offences or allegations against staff or volunteers

In such cases, records must be preserved securely — even beyond normal retention periods — until:

- Statutory limitation periods have passed, OR
- Legal or safeguarding obligations have been satisfied, OR
- A formal decision is taken by the IGA Safeguarding / Data-Protection Lead to archive and review rather than destroy

The decision to suspend disposal must be documented, with rationale and review date.

Governance, Roles & Responsibilities for Disposal

The following roles are responsible for ensuring proper disposal procedures:

- Club Safeguarding Lead / Welfare Officer — initiates review of records eligible for destruction; verifies no ongoing or future safeguarding need exists
- Data Protection Officer (DPO) or equivalent — authorises destruction, maintains destruction log, oversees secure deletion or shredding methods
- IGA Central Safeguarding / Data-Protection Team — periodically audits club disposal logs and compliance, ensures standards are consistent across jurisdictions
- All staff with access to sensitive records — must report any known or suspected unauthorised retention or improper disposal

Destruction must not be delegated to persons without appropriate clearance or training in data protection and safeguarding confidentiality.

Roles & Responsibilities

Effective safeguarding data management relies on clear accountability. This section outlines the responsibilities of all individuals and groups involved in processing safeguarding, welfare, and personal data affiliated with the Independent Gymnastics Association (IGA).

1. IGA Board of Directors

- Has overarching responsibility for ensuring compliance with safeguarding and data-protection legislation across all jurisdictions
- Approves the Safeguarding & Data Retention Policy and all major updates
- Ensures sufficient resources are available for compliance, secure systems, controls, and oversight
- Holds ultimate accountability for any serious data breaches or systemic failings

2. IGA Safeguarding Lead / Safeguarding Management Team

- Acts as the organisational lead for safeguarding record handling, retention, access, disposal, and compliance
- Provides guidance and support to clubs on storage, data-sharing, lawful disclosure, and retention decisions
- Oversees auditing and quality assurance of safeguarding data practices across IGA-affiliated organisations
- Acts as point of escalation for complex cases, cross-border data transfers, and breaches affecting safeguarding records\

3. IGA Data Protection Officer / Data Protection Lead

- Ensures all processing activities comply with applicable data-protection law
- Maintains the Record of Processing Activities (ROPA), including legal bases and data-sharing arrangements
- Oversees secure systems design and governance for both digital and physical safeguarding data
- Leads breach reporting processes and liaison with statutory supervisory authorities

4. Club Welfare Officers (CWOs) / Safeguarding Officers

- Act as the primary custodians of safeguarding and welfare records within clubs
- Ensure accurate, timely, and secure recording of safeguarding concerns, communication, referrals, and outcomes
- Control and monitor access on a strict need-to-know basis
- Maintain local retention and destruction logs and initiate review of records reaching end of retention period
- Support coaches, staff, and volunteers in correct data handling and reporting
- Escalate serious concerns and high-risk data-sharing decisions to IGA leads

5. Club Owners / Senior Managers

- Ensure club-level implementation of the policy and secure storage infrastructure
- Assign local roles (e.g. CWO) and ensure those responsible are trained and competent
- Ensure onboarding and training includes confidentiality and safeguarding data procedures
- Cooperate fully in audits and compliance checks by IGA

6. Coaches, Technical Staff & Volunteers

- Must record and report safeguarding concerns immediately using club safeguarding procedures
- Must maintain confidentiality — only sharing information with authorised safeguarding personnel
- Must comply with secure handling rules when creating, storing or transmitting welfare information
- Must undertake required safeguarding and data-protection training

7. External Service Providers & Third-Party Data Processors

Where clubs engage third parties (e.g., database providers, cloud hosting, physiotherapy services):

- They must be contracted under compliant data-processing agreements
- They must follow all data-security and confidentiality requirements as defined by applicable laws and this policy
- Clubs remain responsible for ensuring third-party compliance and oversight

8. All Personnel

Everyone working within or supporting IGA must:

- Treat safeguarding and personal data as highly confidential
- Report any concerns regarding mishandling, loss, or unauthorised access immediately
- Follow procedures for secure communication and documentation
- Complete mandatory safeguarding and confidentiality training

Summary of Accountability

Role	Primary Accountability
IGA Board	Governance, compliance assurance
IGA Safeguarding Lead	Safeguarding records oversight
IGA DPO / DP Lead	Data protection compliance & breach management
Club Welfare Officer	Day-to-day safeguarding data custody
Coaches & Volunteers	Accurate reporting & secure handling
Third-Party Providers	Contracted compliance with standards

Data Breach Management & Reporting

Given the sensitive nature of safeguarding, welfare, health, and child-protection data held by IGA and its clubs, any breach — accidental or deliberate — must be treated with the highest seriousness. A robust, transparent, and timely breach-response procedure is essential to protect affected individuals, meet statutory obligations, and maintain trust.

This section defines responsibilities, processes, and timelines for detection, containment, reporting, and remediation of data breaches involving safeguarding data.

Definition of a Data Breach

A "data breach" under this policy includes, but is not limited to:

- Unauthorized or accidental access to safeguarding or welfare records (paper or digital) by persons without legitimate need
- Loss, theft, or misplacement of paper files containing personal / special-category data
- Unauthorised or accidental disclosure of data (e.g. sending safeguarding information to wrong recipient, sharing by insecure means, improper publishing)
- Loss or compromise of digital data (e.g. hacking, ransomware, inadvertent deletion, unprotected backups, insecure cloud storage, inadequate encryption)
- Any event where confidentiality, integrity, or availability of safeguarding data is compromised

Immediate Response & Containment

When a breach is suspected or discovered, the following steps must be taken without delay:

1. Containment
    - Secure or lock down the affected records, systems, or storage (remove access, isolate systems, disable accounts, secure physical files)
    - Prevent further unauthorised access or disclosure
2. Initial Assessment
    - Identify the nature of the breach: what data is involved, how many individuals affected, how the breach occurred, whether data remains at risk
    - Determine scope: whether this is a limited incident or indicates a wider systemic vulnerability
3. Notification of Safeguarding & Data-Protection Leads
    - Immediately inform the responsible officers at club level (e.g. Club Welfare Officer) and escalate to the central IGA Safeguarding / Data Protection Lead
4. Temporary Suspension (if required)
    - Suspend further processing, sharing or access to affected data until security is restored and risk understood

Breach Reporting & Regulatory Obligations

Internal Reporting

- A full report must be compiled including: date/time discovered, nature of breach, data involved, number/type of individuals affected, estimated risk, containment actions, and proposed remediation.
- The report should be stored securely, separate from general records, and access restricted to authorised safeguarding/data-protection officers.

External Reporting (if required)

Depending on severity, regulatory obligations, and local law, IGA or responsible club must:

- Report to the relevant supervisory authority (e.g. Information Commissioner's Office (ICO) in the UK; equivalent authority in Channel Islands / Ireland) without undue delay, and where feasible within statutory timeframes (e.g. within 72 hours for "likely risk to rights and freedoms" under GDPR/UK GDPR)

- Notify affected individuals (or, for minors, their parent/guardian) if breach poses high risk to their rights, welfare or privacy — unless doing so itself would risk further harm (e.g. in safeguarding investigations)
- Where breach involves potential criminal activity, unauthorised access, or risks to child protection — consider reporting to law enforcement or child-protection agencies

Coordination with Safeguarding Processes
If breach overlaps with safeguarding risks — e.g. unauthorised sharing of sensitive health or abuse-related data — ensure safeguarding procedures are triggered in parallel (e.g. welfare assessment, risk mitigation, support to affected individuals).

Remediation, Recovery & Prevention
After initial containment and reporting:
- Restore secure storage or access systems (encryption, updated access controls, secure backups, restricted permissions)
- Review and revise policies, procedures, and access controls as needed to prevent recurrence
- Provide training or retraining to staff regarding data-protection, confidentiality, breach awareness, and handling safeguarding data
- Where appropriate, offer support to affected individuals (physical, psychological, welfare support) and document all actions taken

Documentation & Audit Trail
All breach-related activities must be documented comprehensively, including:
- Incident report (what, when, how)
- Containment and remediation actions and timeline
- Notifications sent (to authorities, individuals)
- Decisions made (why or why not to notify, data destroyed or recovered)
- Follow-up reviews and audit findings
- Lessons learned and policy or procedural changes implemented

These records must be kept securely and indefinitely (or until final resolution of any legal/regulatory obligations) — even if original data was destroyed, to enable accountability and external review if required.

Roles & Responsibilities
- Club Welfare Officer / Data-Protection Lead — detect and report breaches at club level; lead immediate containment; notify IGA central lead.
- IGA Data-Protection Officer / Safeguarding Lead — coordinate cross-club response; assess need for external reporting; oversee remediation, recovery, audits and policy updates.
- All staff, volunteers, external providers — required to report any suspected or actual breach immediately; cooperate with investigations; follow all containment instructions.
- IGA Board — ensure resources, oversight, and remedial support; review breach incidents and systemic risks; approve policy changes if needed.

Training & Preparedness

To reduce risk of breaches and ensure effective response:

- All staff with access to safeguarding data must receive regular training on data-protection, confidentiality, secure handling, and breach protocols
- Clubs must maintain incident-response plans that are tested periodically (e.g. tabletop exercises, drills)
- Secure systems (physical and digital) should be reviewed and updated to keep pace with best practice — encryption standards, access controls, logging, backup security

Transparency and Learning

IGA commits to:

- Reviewing each breach to identify root causes and system weaknesses
- Sharing aggregated lessons learned (without breaching confidentiality) with clubs to improve safeguarding and data-protection culture
- Updating this policy when necessary to reflect lessons, legal changes, or improved practices

Training, Audit & Compliance Monitoring

To ensure the effective implementation of this Safeguarding & Data Retention Policy — and to protect gymnasts, staff, and the organisation — IGA mandates regular training, auditing, and compliance monitoring. These mechanisms help detect non-compliance early, support continuous improvement, and ensure accountability across all clubs and jurisdictions.

Mandatory Training Program

All relevant personnel must undergo training appropriate to their role.

Who Must Be Trained

- Club Welfare Officers / Safeguarding Officers
- Coaches, technical staff, volunteers working with gymnasts (including minors)
- Administrative staff involved in record-keeping, data entry, or data management
- Data Protection Officers or persons with responsibilities for data security
- Any third-party providers or contractors engaged in processing safeguarding or welfare data

Training Content & Frequency

Training must cover:

- Key concepts: safeguarding, confidentiality, data protection, special-category data, data subject rights
- Handling of safeguarding records: storage, access control, data minimisation, secure destruction
- Procedures: reporting concerns, data-sharing protocols, data-breach response, consent management
- Legal & regulatory obligations relevant to all jurisdictions covered (UK, Channel Islands, Ireland)
- Ethical responsibilities: respect for gymnast privacy, dignity, autonomy, and welfare

Training must be provided:

- On induction (when a person first assumes a relevant role)
- At regular intervals — at least every 2 years, or sooner if there are changes to the policy or relevant legislation
- Whenever a breach, incident, or serious near-miss occurs — to reflect lessons learned

Records of Training

Clubs must keep:

- Completed training records (who, role, date, scope of training)
- A training log or register as part of safeguarding compliance documentation
- Evidence that staff have accepted and understood their duty under this policy

Internal Audits & Compliance Checks

To maintain standards and verify adherence, regular audits must be conducted across all IGA-affiliated clubs.

Audit Frequency & Scope

- Annual audits at minimum. More frequent (e.g. quarterly) reviews may be needed for high-risk clubs or where historical issues have arisen.
- Audit scope must include:
  - Review of storage, access controls, and secure handling of safeguarding data
  - Verification of retention schedules and destruction logs — ensuring old records are disposed of securely when appropriate
  - Review of data-sharing logs and multi-agency agreements
  - Assessment of access permissions and role-based access control enforcement
  - Verification of training records, staff roles, and compliance with confidentiality requirements

Audit Process & Responsibilities

- Club-level audits are led by the Club Welfare Officer or designated compliance lead.
- Central IGA oversight team (Safeguarding / Data-Protection Lead) should perform spot-check audits across clubs, especially those operating in multiple jurisdictions or with large memberships.
- Audits must result in a formal report summarising findings, compliance gaps or risks, required remedial actions, deadlines, and responsible persons.

Follow-up and Remediation

- Clubs must implement corrective actions within a defined timeframe (e.g. 30–90 days, depending on severity)
- Failure to remedy significant non-compliance may lead to escalation to IGA central governance, including possible sanctions or suspension of club affiliation
- All findings, remediation actions, and follow-up must be logged and retained for audit trail

Monitoring of Data-Protection Compliance & Breach Management
In addition to audits, continuous monitoring is required to manage data-protection risks and respond swiftly to incidents:

- Logging and review of data access events — who accessed what records, when, and for what purpose
- Monitoring of data-sharing events and cross-jurisdiction transfers to ensure lawful basis, security, and documentation
- Review of backup, storage, and deletion processes to prevent unauthorised retention or data leaks
- Periodic testing of security systems (digital encryption, cloud-hosting compliance, physical lockups, disposal procedures)

Where weaknesses are identified, immediate action is required, and follow-up audits scheduled to verify resolution.

Reporting, Oversight & Accountability

- Clubs must submit annual compliance reports to the central IGA Safeguarding/Data-Protection Lead, summarising audits, incidents, training records, and outstanding actions
- The IGA Board will review compliance reports periodically to ensure organisation-wide adherence and allocation of resources for improvements
- Any data-protection breach, safeguarding incident, near-miss or risk identified during audit must be escalated immediately according to the Data Breach Management protocol

Continuous Improvement & Policy Review

- Feedback from audits, staff, gymnasts, and external agencies should feed into periodic policy review cycles
- Where legislation, best practice guidance, or safeguarding standards change, IGA will update the policy — and retrain all relevant personnel accordingly
- Clubs must incorporate an annual lessons-learned review, evaluating whether practices remain effective and identifying areas for enhancement

Policy Review & Version Control

Purpose of Review
To ensure the Safeguarding & Data Retention Policy remains fully compliant with:

- Current data-protection legislation across all jurisdictions in which IGA operates
- National safeguarding standards and best practice guidance
- Technological and operational changes affecting data security
- Lessons learned from audits, incidents, or reported concerns

Regular reviews help maintain the highest standards of protection for gymnasts and ensure consistent, lawful data-handling practices across all IGA-affiliated clubs.

Review Frequency

- Formal review every 2 years as a minimum
- Interim review required earlier if any of the following occur:
  - Legislative or regulatory changes (e.g. amendments to UK GDPR / national data-protection laws)
  - Updates to national safeguarding frameworks
  - Significant data breach or safeguarding incident indicating policy weaknesses
  - Introduction of new systems, technologies, or working practices related to data processing

Roles & Responsibilities for Policy Review

Role	Responsibility
IGA Safeguarding Lead	Leads content review and consultation with stakeholders
IGA Data Protection Lead / DPO	Ensures compliance with relevant data-protection law
IGA Board of Directors	Approves revised versions prior to publication
Club Welfare Officers	Provide feedback from club-level implementation
Coaches & Staff	Contribute insights on practical improvements in everyday use

Communication & Implementation of Updates

When updates are approved:

- A new version will be circulated to all clubs with a clear summary of changes
- All organisations must cease using superseded versions immediately
- Staff must acknowledge receipt and complete additional training if required
- Clubs must update references in local procedures, handbooks, and privacy notices
- New and updated materials should be published on internal/external platforms where required (e.g. IGA member portals)

Reporting Concerns or Complaints about Data Handling

Purpose of Reporting

IGA is committed to a transparent, accountable culture in which any individual — gymnast, parent/guardian, staff member, volunteer, or external stakeholder — can raise a concern if they believe:

- Safeguarding or welfare data has been mishandled
- Confidential information has been accessed or shared inappropriately

Purpose of Reporting
IGA is committed to a transparent, accountable culture in which any individual — gymnast, parent/guardian, staff member, volunteer, or external stakeholder — can raise a concern if they believe:

- Safeguarding or welfare data has been mishandled
- Confidential information has been accessed or shared inappropriately
- Data has been stored or retained insecurely
- There is a breach of this policy or any applicable data-protection legislation
- A request relating to personal data has not been handled lawfully or fairly

All concerns will be taken seriously and handled promptly.

How to Raise a Concern
Concerns may be raised through any of the following routes:

1. Club Welfare Officer / Safeguarding Lead — first point of contact for local issues
2. Club Data Protection Contact — where concern relates specifically to storage, security or handling
3. IGA Safeguarding Team — for issues that cannot be resolved at club level
4. IGA Data Protection Lead / Officer — for matters involving significant risk or policy non-compliance

Concerns should be submitted as soon as possible after the incident, preferably in writing, describing what occurred, when, who was involved, and any perceived risks.

Anonymous reports will be accepted and investigated to the fullest extent possible.

Response & Investigation Process
Upon receiving a concern or complaint:

- Acknowledgement will be issued promptly (typically within 5 working days)
- The issue will be assessed to determine urgency, risk, and potential breach
- Where safeguarding risk is present, safeguarding procedures take precedence
- Investigation will be conducted impartially by an appropriate person not involved in the incident
- Outcomes will be documented and shared appropriately with the reporting party, respecting confidentiality limits

Depending on severity, escalation may include:

- Central IGA oversight
- External safeguarding agencies
- Data-protection supervisory authorities
- Law enforcement

Protection for Whistleblowers
No person will be penalised for raising a concern in good faith.
IGA will ensure:

- Concerns can be raised without fear of retaliation
- Identities are protected as far as legally and operationally possible
- Individuals are supported throughout the process

Escalation to Regulators
If a reporting party believes:

- A complaint has not been handled appropriately, or
- There is a serious or ongoing breach of data-protection law

They have the right to contact the relevant supervisory authority in their jurisdiction (e.g. the Information Commissioner's Office (ICO) in the UK, or equivalent regulators in the Channel Islands or Republic of Ireland).

Details will be provided in the Useful Contact Information section of this policy.

Record Keeping
All concerns, investigations, and outcomes must be:

- Logged securely
- Retained according to this policy's retention rules
- Reviewed periodically to identify systemic issues and lessons learned

Trends and recurring issues will inform policy review and staff training priorities.