



PRIVACY NOTICE

Approved by: Andrew Banks – CEO and Chief Instructor

Version: 2.0

Replaces: KRMA Privacy Policy dated 20 July 2023

Effective date: 14 July 2026

Next review date: 14 July 2027

+44 01652 653560

www.KRMA.co.uk

admin@krma.co.uk

Unit 22 Island Carr Road,
Brigg,
North Lincolnshire,
DN20 8PD

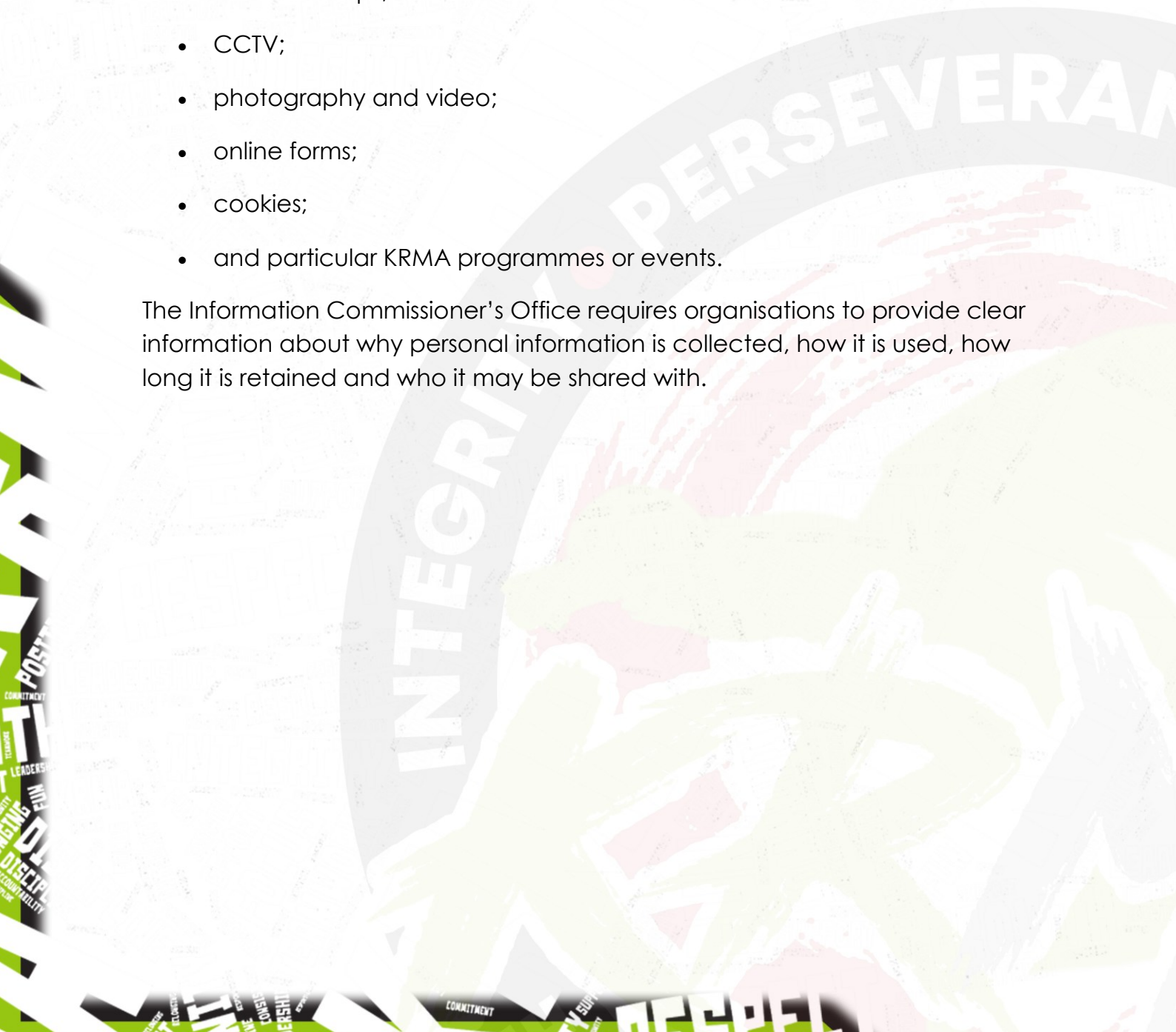
Important Information

This Privacy Notice explains how Koku-Ryu Martial Arts collects, uses, stores, shares and protects personal information.

It should be read alongside any more specific privacy information provided in connection with:

- employment;
- volunteering;
- recruitment;
- competitions;
- residential trips;
- CCTV;
- photography and video;
- online forms;
- cookies;
- and particular KRMA programmes or events.

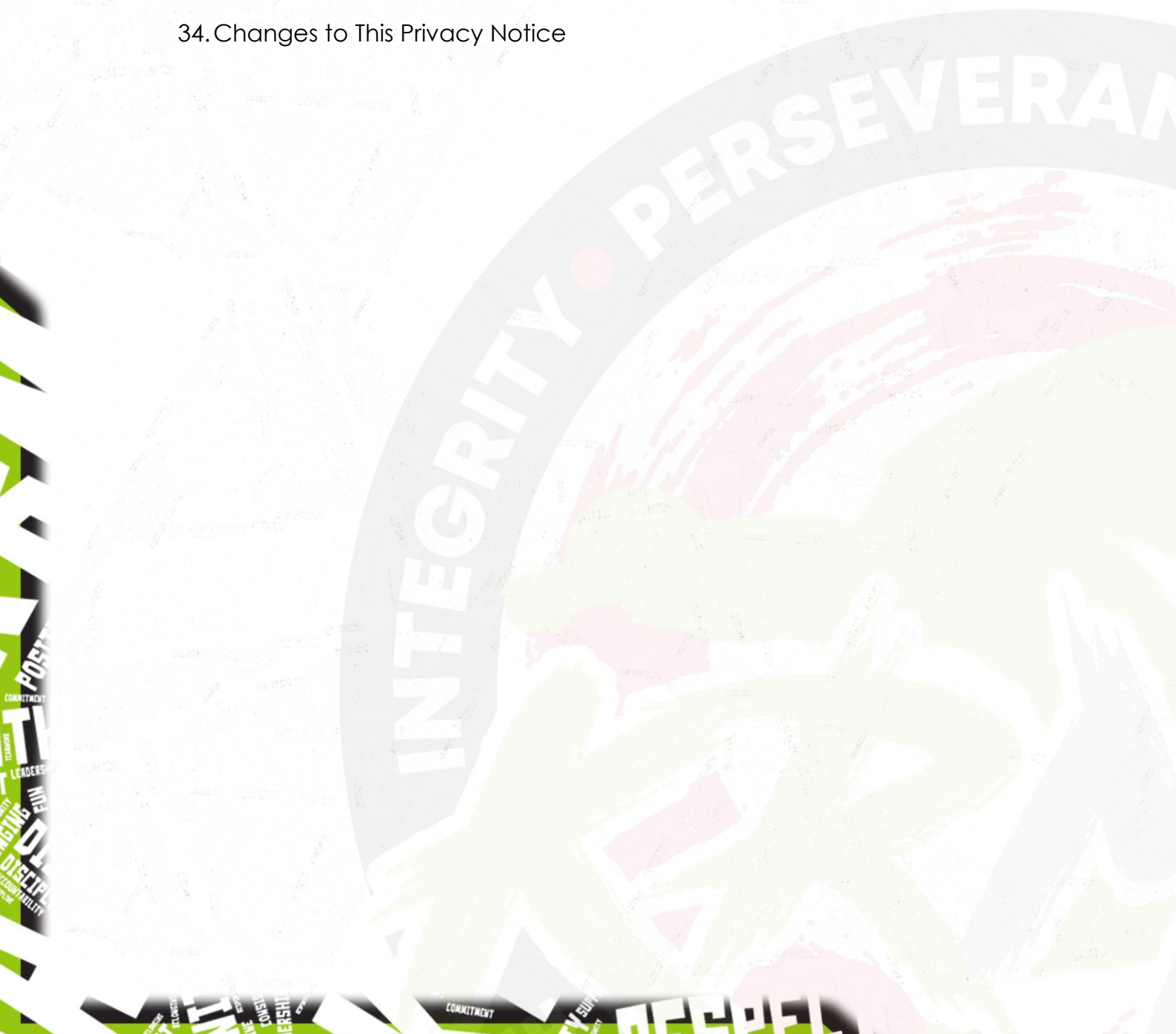
The Information Commissioner's Office requires organisations to provide clear information about why personal information is collected, how it is used, how long it is retained and who it may be shared with.



Contents

1. Who We Are
2. How to Contact Us
3. Who This Privacy Notice Applies To
4. Our Data-Protection Commitment
5. Personal Information We Collect
6. Special Category and Sensitive Information
7. Information About Children
8. How We Collect Personal Information
9. Why We Use Personal Information
10. Our Lawful Bases
11. Enquiries, Trials and Membership Administration
12. Attendance, Progress, Grading and Achievement Records
13. Medical Information and Reasonable Adjustments
14. Safeguarding and Welfare Information
15. Payments, Accounts and Financial Records
16. Communications and Marketing
17. Photographs, Video and Media
18. CCTV and Security
19. Competitions, Events, Travel and Residential Activities
20. Websites, Cookies and Online Services
21. Staff, Volunteers, Contractors and Applicants
22. Who We Share Information With
23. Safeguarding and Emergency Information Sharing
24. Service Providers and Data Processors

- 25. International Transfers
- 26. How We Protect Information
- 27. How Long We Retain Information
- 28. Your Data-Protection Rights
- 29. Children's Rights and Requests by Parents
- 30. Withdrawing Consent
- 31. Automated Processing and Artificial Intelligence
- 32. Personal Data Breaches
- 33. Complaints and the Information Commissioner
- 34. Changes to This Privacy Notice



1. Who We Are

Koku-Ryu Martial Arts, referred to throughout this Notice as “**KRMA**”, “**we**”, “**us**” or “**our**”, provides martial arts, fitness, education, competition, community and personal-development programmes.

For most of the personal information described in this Notice, KRMA acts as the **data controller**.

This means that KRMA decides:

- why the information is needed;
- what information should be collected;
- how it will be used;
- who it may be shared with;
- how long it will be retained;
- and how it will be protected.

Some organisations that work with KRMA may act as:

- processors acting on our instructions;
- independent data controllers;
- or joint controllers with KRMA.

Where another organisation makes its own decisions about personal information, it may provide its own Privacy Notice.

2. How to Contact Us

Questions, concerns and data-protection requests may be directed to:

Koku-Ryu Martial Arts

Unit 22 Island Carr Road
Brigg
North Lincolnshire
DN20 8PD

Email: admin@krma.co.uk

Telephone: 01652 653560

Please mark written or emailed requests:

For the attention of the Data Protection Lead

Safeguarding concerns should normally be directed to:

Designated Safeguarding Lead: Kayleigh Humphreys

Email: safeguarding@krma.co.uk

Telephone: 01652 653560

Where someone is in immediate danger, call **999**.



3. Who This Privacy Notice Applies To

This Notice may apply to:

- prospective students;
- trial participants;
- current students;
- former students;
- parents and carers;
- emergency contacts;
- authorised collectors;
- adult members;
- competition participants;
- event attendees;
- scholarship applicants and recipients;
- private-lesson clients;
- website visitors;
- mailing-list subscribers;
- school and community contacts;
- suppliers;
- contractors;
- instructors;
- employees;
- volunteers;
- junior instructors;
- job applicants;
- visitors;

- complainants;
- witnesses;
- and anyone else who communicates or interacts with KRMA.

Staff, volunteers and applicants may receive additional privacy information explaining employment and recruitment processing in greater detail.



4. Our Data-Protection Commitment

KRMA is committed to handling personal information:

- lawfully;
- fairly;
- transparently;
- accurately;
- securely;
- and only for legitimate purposes.

We will aim to:

1. Explain why information is being collected.
2. Collect only what is reasonably necessary.
3. Use an appropriate lawful basis.
4. protect sensitive information carefully.
5. restrict access according to role.
6. avoid unnecessary disclosure.
7. retain information only for an appropriate period.
8. respect individual data rights.
9. respond promptly to mistakes and security incidents.
10. consider children's best interests.
11. use reputable suppliers and systems.
12. review our privacy arrangements regularly.

We do not sell personal information.

We will not use confidential:

- medical;
- safeguarding;

- employment;
- financial;
- or criminal-record information

for unrelated publicity or marketing.



5. Personal Information We Collect

The information collected depends upon the person's relationship with KRMA and the services involved.

5.1 Identity information

This may include:

- full name;
- previous name where required;
- preferred name;
- title;
- date of birth;
- age;
- gender information where relevant;
- photograph;
- signature;
- membership number;
- and identity documentation.

5.2 Contact information

This may include:

- home address;
- email address;
- telephone number;
- parent or carer details;
- emergency contacts;
- authorised collectors;
- and preferred communication method.

5.3 Membership information

This may include:

- programme;
- venue;
- class allocation;
- joining date;
- membership status;
- attendance;
- belt or grade;
- uniform information;
- equipment requirements;
- private lessons;
- and participation history.

5.4 Training and development information

This may include:

- assessments;
- grading results;
- instructor feedback;
- tags;
- development plans;
- competition results;
- leadership progress;
- achievements;
- certificates;
- and formal qualifications.

5.5 Health and support information

This may include:

- medical conditions;
- disability;
- allergies;
- injuries;
- medication;
- pregnancy;
- emergency treatment requirements;
- SENDI;
- sensory needs;
- communication needs;
- mobility;
- reasonable adjustments;
- personal-care requirements;
- and participation restrictions.

5.6 Safeguarding and welfare information

This may include:

- concerns;
- disclosures;
- allegations;
- referrals;
- missing-child incidents;
- bullying reports;
- behaviour records;
- injury information;

- statutory-agency communication;
- risk assessments;
- and protection plans.

5.7 Family and collection information

This may include:

- parental-responsibility information;
- collection arrangements;
- passwords;
- court orders;
- contact restrictions;
- family circumstances relevant to safety;
- and independent-travel permission.

5.8 Financial information

This may include:

- membership fees;
- invoices;
- payment status;
- transaction references;
- direct-debit details;
- refunds;
- discounts;
- purchases;
- scholarship information;
- and financial correspondence.

Payment information may be processed directly by an authorised payment provider rather than stored fully by KRMA.

5.9 Communication information

This may include:

- emails;
- telephone notes;
- text messages;
- approved messaging history;
- online-form responses;
- complaints;
- feedback;
- social-media communication;
- and meeting notes.

5.10 Photographs and recordings

This may include:

- class photographs;
- grading photographs;
- competition footage;
- achievement photographs;
- promotional recordings;
- educational footage;
- CCTV images;
- and authorised audio recordings.

5.11 Online and technical information

This may include:

- IP address;
- browser;

- device type;
- website activity;
- online account information;
- access logs;
- cookie information;
- form submissions;
- and communication preferences.

5.12 Event and travel information

This may include:

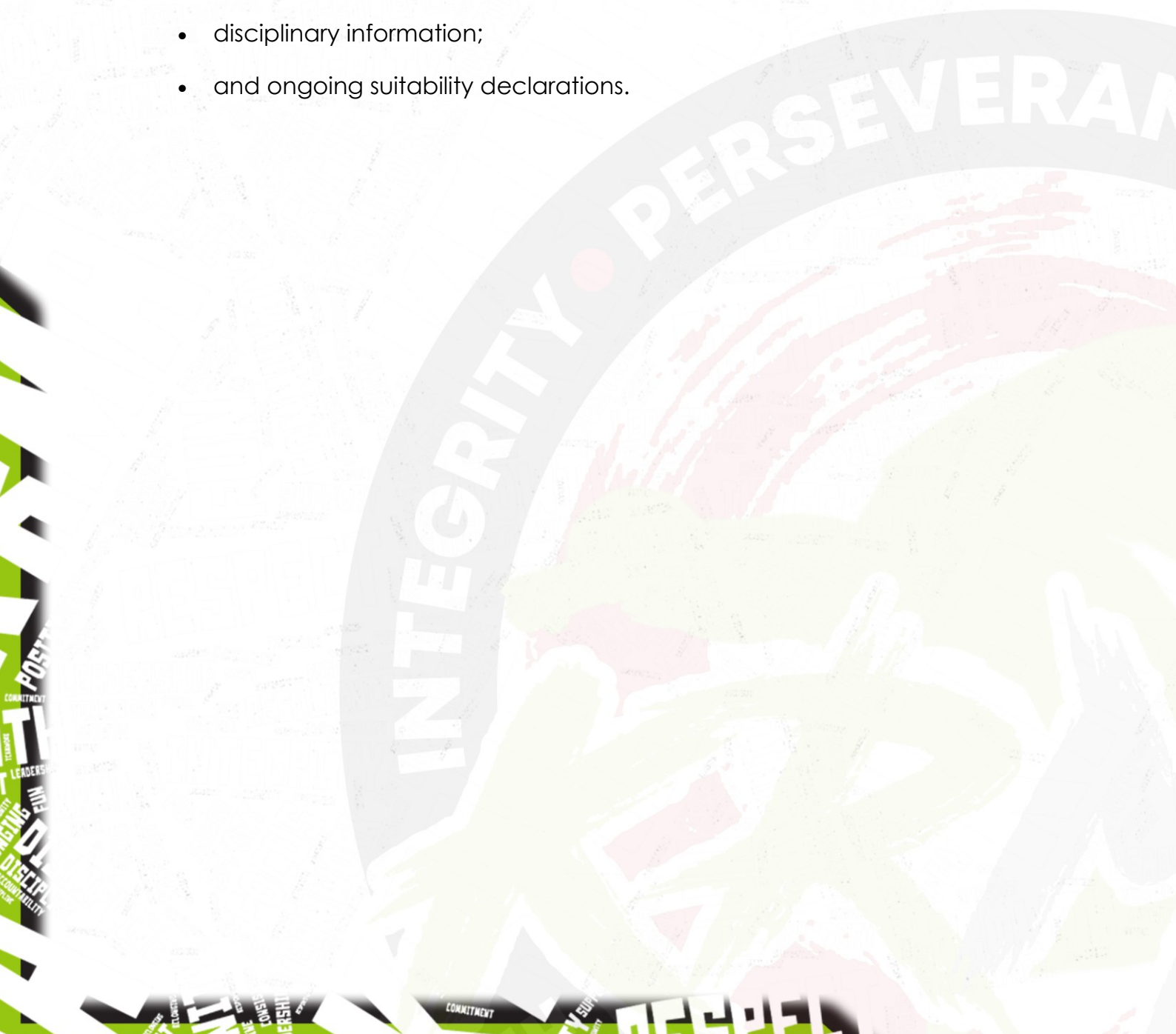
- competition entries;
- event bookings;
- emergency contacts;
- transport allocation;
- accommodation;
- dietary requirements;
- passport information where necessary;
- insurance information;
- rooming arrangements;
- and travel consent.

5.13 Employment, volunteering and recruitment information

This may include:

- application forms;
- employment history;
- references;
- interview notes;

- qualifications;
- martial arts grades;
- right-to-work information;
- DBS-check records;
- training;
- performance;
- attendance;
- payroll;
- health and adjustment information;
- disciplinary information;
- and ongoing suitability declarations.



6. Special Category and Sensitive Information

Some information requires additional protection.

This includes information concerning:

- health;
- disability;
- racial or ethnic origin;
- religious or philosophical beliefs;
- political opinions;
- trade-union membership;
- genetic information;
- biometric identification;
- sexual orientation;
- and sex life.

KRMA most commonly processes special category information relating to:

- medical conditions;
- injuries;
- disability;
- SENDI;
- pregnancy;
- allergies;
- medication;
- reasonable adjustments;
- and safeguarding.

We will only process this information where:

- it is genuinely necessary;

- an appropriate lawful basis applies;
- an additional special-category condition applies;
- access is restricted;
- and suitable protection is in place.

Depending upon the circumstances, KRMA may rely upon conditions connected with:

- explicit consent;
- employment obligations;
- vital interests;
- legal claims;
- safeguarding;
- substantial public interest;
- or the protection of someone's health, welfare or safety.

Medical and support information will normally be shared only with people who require it to:

- make participation safe;
- provide an adjustment;
- respond to an emergency;
- or fulfil a safeguarding or legal responsibility.

7. Information About Children

A significant proportion of KRMA students are children.

Children's information requires particular protection because children may:

- understand privacy risks less fully;
- find it harder to challenge adults;
- be more vulnerable to inappropriate contact or publicity;
- and experience long-term effects from information shared about them.

KRMA will consider:

- the child's age;
- maturity;
- understanding;
- best interests;
- safety;
- privacy;
- wishes;
- and ability to exercise their own rights.

The ICO's current guidance requires organisations to take a child-centred approach and give particular consideration to children's best interests when using their personal information.

7.1 Parents and carers

Parents and carers will normally be involved in:

- enrolment;
- payments;
- emergency arrangements;
- medical information;
- photography choices;

- travel;
- collection;
- and communication.

However, a parent or carer does not automatically own the child's personal information or have an unrestricted right to receive every record.

KRMA may need to consider:

- the child's own rights;
- the child's understanding;
- confidentiality;
- safeguarding;
- parental responsibility;
- court orders;
- and information concerning other people.

7.2 Child-friendly explanations

KRMA will aim to explain important privacy information to children using:

- clear language;
- age-appropriate examples;
- accessible formats;
- visual information where helpful;
- and opportunities to ask questions.

7.3 Children's wishes

Where participation in photography, publicity or another activity is optional, KRMA will consider the child's own wishes.

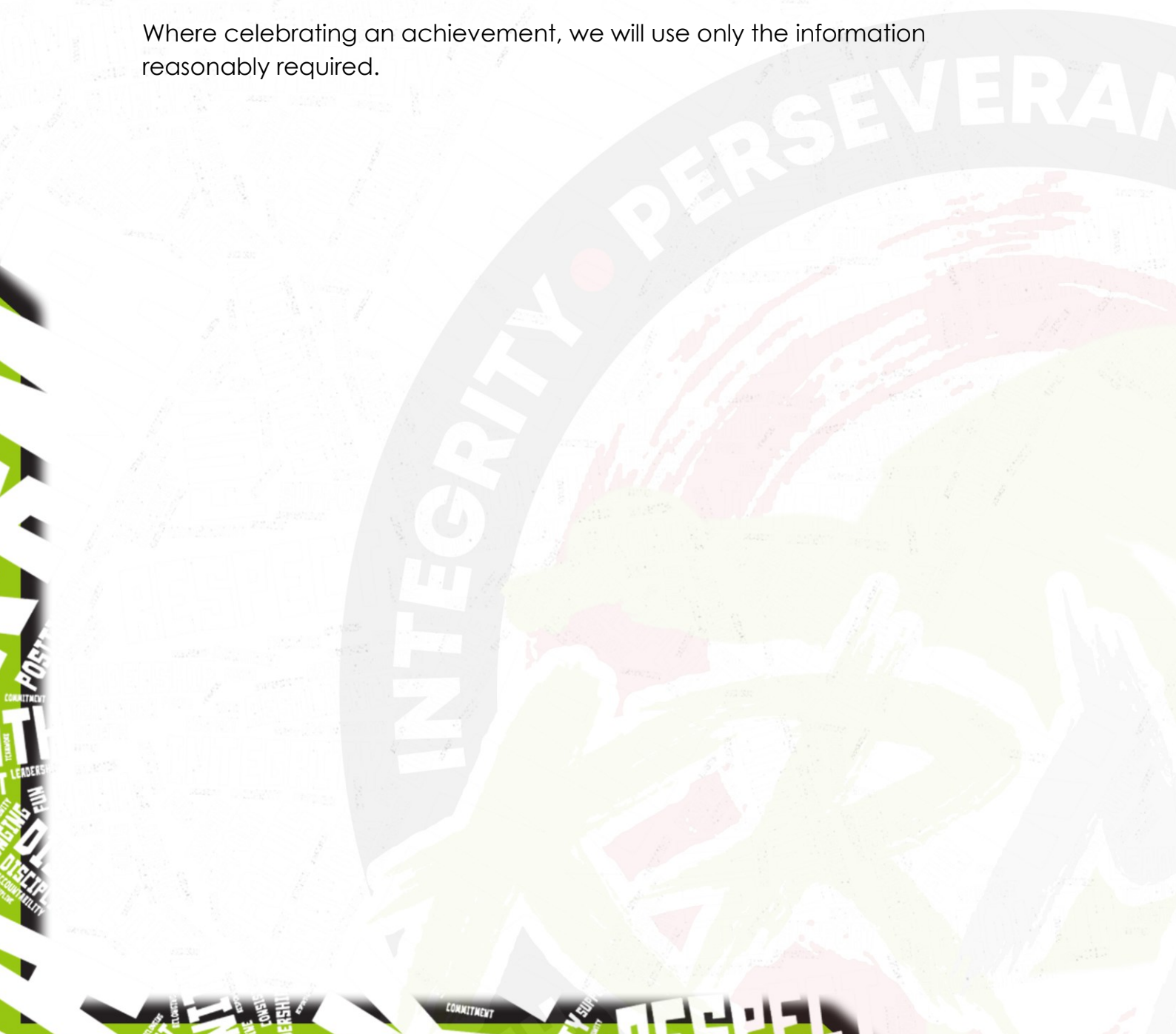
A child who clearly does not wish to be photographed or recorded should not normally be forced to participate merely because an adult previously provided permission.

7.4 Information published about children

KRMA will avoid publicly sharing unnecessary information such as:

- full date of birth;
- home address;
- private telephone number;
- school;
- medical condition;
- safeguarding circumstances;
- collection arrangements;
- or regular travel routines.

Where celebrating an achievement, we will use only the information reasonably required.



8. How We Collect Personal Information

We may collect information directly from:

- the individual;
- a parent or carer;
- an online form;
- membership registration;
- a trial booking;
- an event booking;
- email;
- telephone;
- social media;
- a meeting;
- attendance;
- assessment;
- photography;
- CCTV;
- or observation during an activity.

We may also receive information from:

- another parent or authorised adult;
- an instructor;
- school;
- competition organiser;
- event provider;
- governing or membership body;
- previous martial arts organisation;

- referee;
- former employer;
- Disclosure and Barring Service;
- police;
- local authority;
- healthcare professional;
- insurer;
- payment provider;
- website provider;
- or another organisation where sharing is lawful.

Where we obtain information from another source, we will provide privacy information within the period required by law unless an exemption applies. Privacy information should normally be supplied when information is collected directly, or within a reasonable period where it comes from another source.

9. Why We Use Personal Information

We may use personal information to:

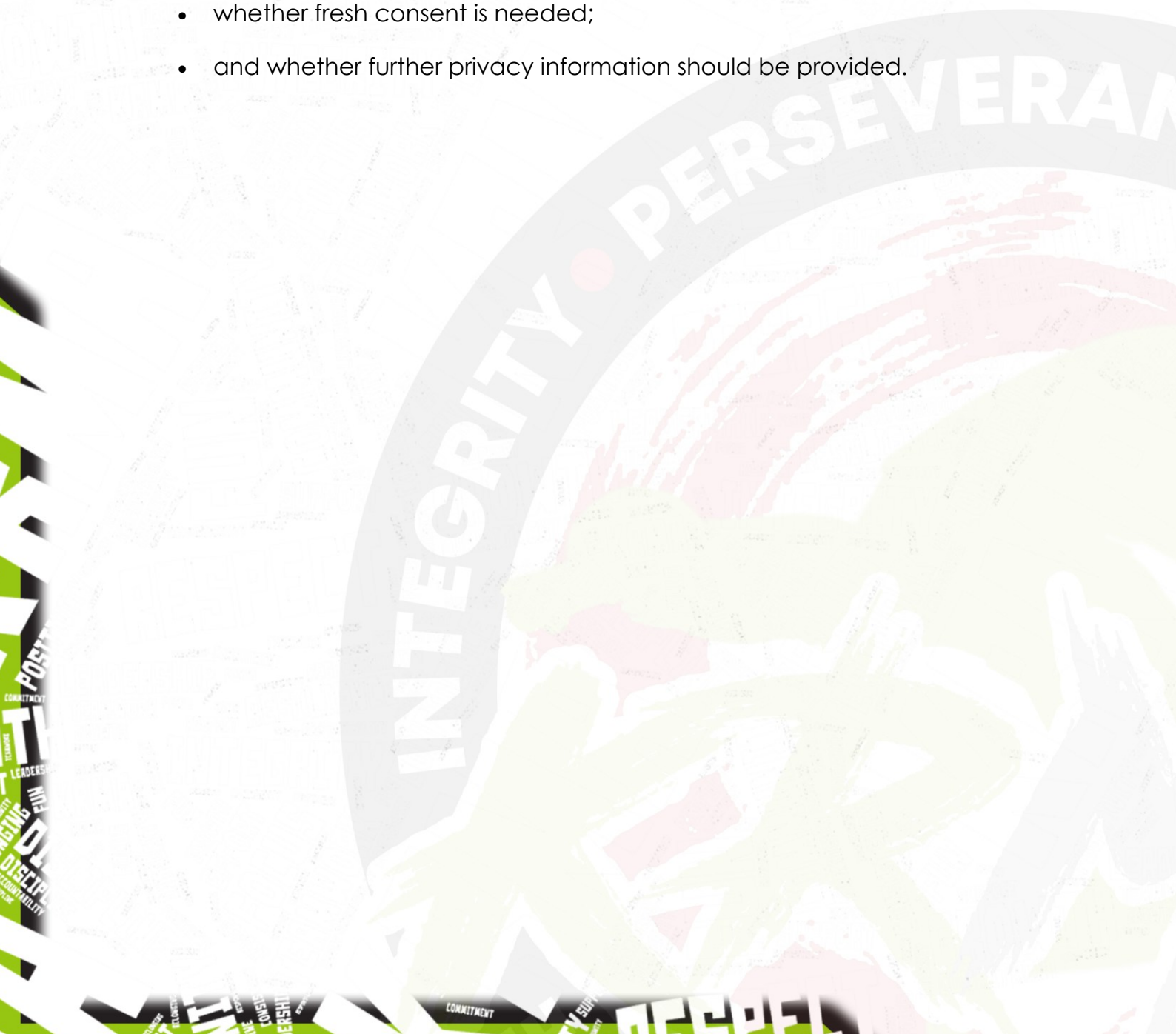
- respond to enquiries;
- arrange trial classes;
- enrol students;
- manage memberships;
- deliver classes and private lessons;
- record attendance;
- assess progress;
- conduct gradings;
- issue certificates;
- organise competitions and demonstrations;
- manage events and trips;
- communicate operational information;
- collect and administer payments;
- provide reasonable adjustments;
- respond to medical emergencies;
- protect children and adults at risk;
- investigate complaints;
- manage behaviour;
- prevent fraud;
- protect premises;
- manage staff and volunteers;
- recruit suitable people;
- maintain insurance and legal records;

- promote KRMA where appropriate;
- improve programmes;
- maintain systems and security;
- and comply with legal or regulatory requirements.

We will not automatically use information collected for one purpose for an unrelated purpose.

Where we intend to introduce a materially different use, we will consider:

- whether it is compatible with the original purpose;
- whether another lawful basis is required;
- whether fresh consent is needed;
- and whether further privacy information should be provided.



10. Our Lawful Bases

Data-protection law requires KRMA to identify an appropriate lawful basis for each purpose.

The applicable basis depends upon the information and reason for using it.

10.1 Contract

We may use information because it is necessary to:

- provide requested classes or services;
- administer membership;
- manage bookings;
- provide private lessons;
- process payments;
- deliver events;
- or take steps requested before someone joins.

10.2 Legal obligation

We may process information because the law requires us to do so.

This may include:

- financial and tax records;
- employment records;
- right-to-work checks;
- safeguarding referrals;
- health and safety;
- statutory accident reporting;
- responding to courts;
- and regulatory obligations.

10.3 Legitimate interests

We may use information where KRMA or another organisation has a genuine legitimate interest and the person's rights do not override it.

Possible examples include:

- routine operational communication;
- maintaining attendance and progress records;
- improving services;
- protecting premises;
- preventing fraud;
- managing complaints;
- enforcing agreements;
- and defending legal claims.

Where legitimate interests are relied upon, we will consider:

- the purpose;
- necessity;
- reasonable expectations;
- potential impact;
- safeguards;
- and, particularly for children, their best interests.

10.4 Consent

We may rely upon consent for optional activities such as:

- certain promotional photographs;
- testimonials;
- optional publicity;
- and some direct marketing.

Consent must be:

- informed;

- specific;
- freely given;
- recorded;
- and capable of being withdrawn.

10.5 Vital interests

We may use or share information where necessary to protect someone's life.

This may apply during:

- a serious medical emergency;
- a missing-child emergency;
- or another immediate danger.

10.6 Public task

KRMA will only rely upon public task where we are carrying out a specific function or task established by law.

Operating a beneficial community programme does not, by itself, mean that the public-task basis applies.

10.7 Recognised legitimate interests

Data-protection legislation also permits certain processing under legally defined recognised legitimate interests.

KRMA will rely upon this basis only where the processing falls within an applicable statutory category and the required protections are in place. The organisation must remain transparent and explain which recognised interest is being used.

11. Enquiries, Trials and Membership Administration

When someone enquires about KRMA or books a trial, we may collect:

- name;
- age or date of birth;
- contact details;
- parent or carer information;
- programme interests;
- venue preference;
- relevant medical information;
- and communication history.

We use this information to:

- respond to the enquiry;
- recommend an appropriate programme;
- arrange a trial;
- provide safety information;
- follow up the enquiry;
- and complete enrolment where requested.

The lawful bases may include:

- steps requested before entering a contract;
- legitimate interests in responding to enquiries and managing our services;
- consent for optional marketing;
- and special-category conditions where medical information is provided.

Not every enquiry results in membership.

Information relating to unsuccessful or inactive enquiries will be retained only for an appropriate period and will not automatically be used for indefinite marketing.

11.1 Membership records

When someone joins KRMA, we may use their information to:

- create and manage the membership;
- allocate classes;
- provide programme information;
- record attendance;
- manage payments;
- maintain emergency contacts;
- issue relevant communication;
- administer gradings;
- and provide the agreed service.

The principal lawful basis will normally be contract.

Other bases may apply where information is needed for:

- legitimate operational interests;
- legal obligations;
- health and safety;
- safeguarding;
- or emergency protection.

11.2 Contact details

Members and parents are responsible for telling KRMA when important information changes, including:

- telephone number;
- email;
- home address;

- emergency contacts;
- authorised collectors;
- medical information;
- and parental or court arrangements.

KRMA may periodically ask families to confirm that information remains accurate.



12. Attendance, Progress, Grading and Achievement Records

We may maintain records concerning:

- attendance;
- lateness;
- programme participation;
- training history;
- tags;
- assessments;
- scores;
- grading decisions;
- certificates;
- belt progression;
- competition results;
- leadership development;
- and instructor feedback.

We use this information to:

- provide structured training;
- assess readiness;
- monitor progress;
- maintain safety;
- support reasonable adjustments;
- identify attendance concerns;
- administer gradings;
- issue certificates;
- verify achievements;

- and maintain the integrity of KRMA's grading system.

The lawful bases may include:

- contract;
- legitimate interests in managing training and maintaining accurate achievement records;
- and legal or safeguarding obligations where relevant.

12.1 Long-term grade records

KRMA may retain a limited long-term or permanent record of formal grades and qualifications, including:

- student name;
- discipline;
- grade;
- date awarded;
- examiner;
- and certificate number.

This allows KRMA to:

- verify qualifications;
- replace certificates;
- maintain historical records;
- support continued progression;
- and respond to false or disputed grade claims.

Detailed score sheets and routine coaching notes may be retained for a shorter period.

12.2 Sharing achievements

With an appropriate lawful basis or consent where required, KRMA may celebrate achievements through:

- certificates;

- award presentations;
- newsletters;
- websites;
- social media;
- press releases;
- and promotional material.

We will aim to avoid sharing more personal information than is necessary.



13. Medical Information, SENDI and Reasonable Adjustments

KRMA may collect health and support information where it is necessary to:

- determine whether participation is safe;
- prepare appropriate risk controls;
- respond to an emergency;
- provide first aid;
- support medication arrangements;
- make reasonable adjustments;
- understand allergies or medical restrictions;
- support disability, SENDI or sensory needs;
- plan a safe return following injury;
- and protect the welfare of the student or others.

Health information is special category personal information. Its use requires both an appropriate lawful basis and an additional condition for processing special category information.

13.1 Information we may require

Depending upon the programme and circumstances, we may ask for information concerning:

- medical conditions;
- allergies;
- medication;
- disability;
- pregnancy;
- recent injury;
- concussion or head injury;
- mobility;
- communication;

- sensory needs;
- emergency symptoms;
- treatment instructions;
- healthcare advice;
- and temporary or permanent participation restrictions.

We will not normally request complete medical records where a shorter explanation of the relevant condition, risk and required action is sufficient.

13.2 Why information must be accurate

Students, parents, carers, staff and volunteers should tell KRMA when relevant health information changes.

Failure to provide important information may affect our ability to:

- respond safely;
- make appropriate adjustments;
- assess participation;
- or manage an emergency.

Providing information does not guarantee that every requested arrangement can be implemented.

KRMA will consider:

- safety;
- facilities;
- staffing;
- competence;
- the needs of others;
- and whether the proposed adjustment is reasonable and practicable.

13.3 Who may see medical information

Relevant information may be available to:

- authorised instructors;

- first aiders;
- safeguarding personnel;
- event or trip leaders;
- administrators responsible for emergency records;
- and healthcare or emergency professionals where required.

We will normally provide staff with the information they need to act safely rather than unrestricted access to a person's complete medical history.

13.4 Emergency sharing

During an emergency, we may share relevant information with:

- ambulance personnel;
- hospitals;
- police;
- parents or carers;
- venue staff;
- trip leaders;
- or another person responsible for immediate safety.

Where necessary to protect life, we may act under the vital-interests lawful basis.

13.5 Reasonable adjustments

Information may be used to consider adjustments such as:

- adapted instruction;
- alternative communication;
- additional processing time;
- sensory breaks;
- modified exercises;
- accessible formats;

- partner selection;
- equipment adjustments;
- temporary training restrictions;
- and individual support arrangements.

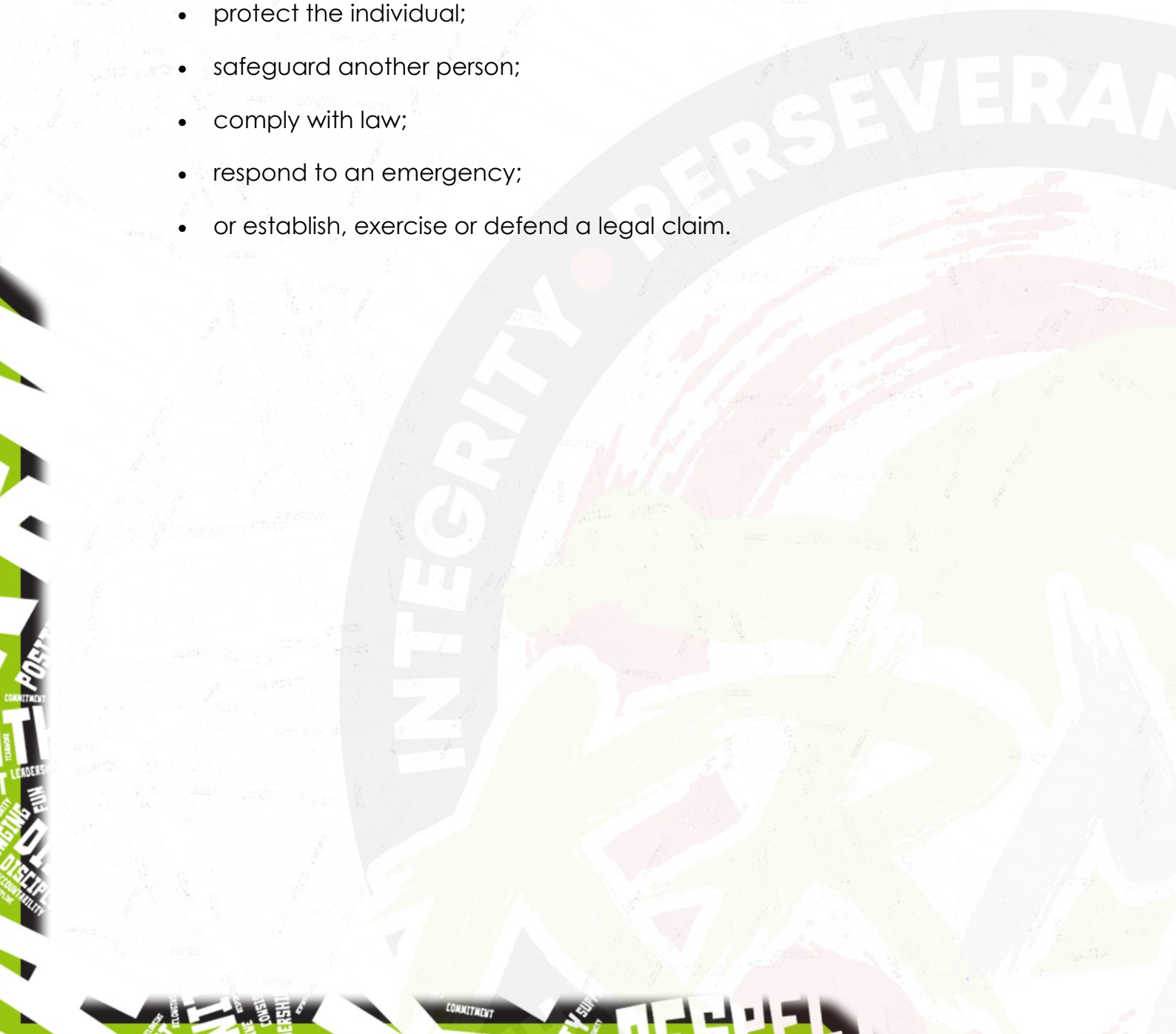
Information concerning an adjustment will not normally be disclosed to other students or families.

13.6 Medical confidentiality and safeguarding

Medical information will normally be treated confidentially.

However, it may be shared without consent where necessary to:

- protect the individual;
- safeguard another person;
- comply with law;
- respond to an emergency;
- or establish, exercise or defend a legal claim.



14. Safeguarding and Welfare Information

KRMA may collect, create and receive personal information where concerns arise about:

- a child;
- an adult at risk;
- a member of staff;
- volunteer;
- instructor;
- parent;
- student;
- or another person connected with KRMA.

Safeguarding information may include:

- disclosures;
- allegations;
- observations;
- incident reports;
- behaviour concerns;
- bullying reports;
- online communication;
- witness information;
- risk assessments;
- photographs or recordings;
- police or local-authority communication;
- and action taken to protect someone.

14.1 Why we process safeguarding information

We may use safeguarding information to:

- protect children and adults at risk;
- assess immediate danger;
- respond to disclosures;
- identify patterns;
- manage allegations;
- make referrals;
- cooperate with statutory agencies;
- impose protective restrictions;
- support affected people;
- and demonstrate that appropriate action was taken.

The lawful bases and additional conditions will depend upon the circumstances and may include:

- legal obligation;
- legitimate interests;
- recognised legitimate interests where applicable;
- vital interests;
- safeguarding of children and individuals at risk;
- substantial public interest;
- employment obligations;
- and legal claims.

14.2 Consent is not always required

KRMA does not always need consent before sharing information for safeguarding purposes.

We may share without consent where:

- someone may be at risk of harm;
- delay could increase the danger;

- seeking consent could alert an alleged perpetrator;
- evidence could be lost;
- the person is unable to consent;
- a statutory agency requires the information;
- or another lawful safeguarding reason applies.

Data-protection law supports necessary, fair and proportionate information sharing to safeguard children.

14.3 Informing the person or family

Where it is safe and appropriate, we will normally explain:

- what information is being shared;
- who it will be shared with;
- and why.

We may delay or withhold this information where notification could:

- increase risk;
- prejudice a police or social-care enquiry;
- expose a confidential source;
- result in retaliation;
- pressure a child;
- or conflict with professional or statutory advice.

14.4 Access to safeguarding records

Safeguarding records are available only to people with an authorised safeguarding or legal need.

They will not normally be disclosed to:

- general instructors;
- uninvolved staff;
- other parents;

- other students;
- or members of unofficial groups.

Safeguarding information will not be used for:

- marketing;
- public relations;
- gossip;
- or resolving unrelated personal disputes.

14.5 Accuracy of safeguarding records

Safeguarding records should distinguish clearly between:

- what was observed;
- what was reported;
- what was alleged;
- what was confirmed;
- professional opinion;
- and action taken.

An allegation will not be recorded as an established fact unless an appropriate finding has been made.

14.6 Retention

Safeguarding records may be retained for longer than ordinary membership information.

Retention will consider:

- the age of the person involved;
- seriousness of the concern;
- involvement of statutory agencies;
- possible future patterns;
- insurance;

- legal advice;
- and applicable safeguarding requirements.



15. Payments, Accounts and Financial Records

KRMA may process financial information to:

- collect membership fees;
- administer direct debits;
- process event and competition fees;
- sell uniforms or equipment;
- issue invoices;
- provide refunds;
- manage scholarships or discounts;
- maintain accounts;
- prevent fraud;
- and comply with tax and financial-record obligations.

15.1 Information processed

This may include:

- account-holder name;
- billing address;
- payment amount;
- payment date;
- payment status;
- transaction reference;
- direct-debit mandate information;
- invoice history;
- refund information;
- debt correspondence;
- and limited information received from payment providers.

15.2 Payment providers

Payments may be processed through an external payment or direct-debit provider.

The provider may act as:

- a processor on KRMA's behalf;
- an independent data controller;
- or both for different elements of the service.

The provider may supply its own Privacy Notice explaining how it uses payment and identity information.

15.3 Card information

KRMA will avoid retaining complete card information where payment can be handled securely by an authorised provider.

Staff must not request that complete card details are sent through:

- ordinary email;
- social-media messages;
- open messaging groups;
- or other insecure channels.

15.4 Failed or overdue payments

Where a payment fails or an account becomes overdue, we may use contact and financial information to:

- notify the account holder;
- resolve an administrative error;
- arrange payment;
- enforce the membership agreement;
- or recover a legitimate debt.

We will not publicly disclose an individual's payment status.

15.5 Financial retention

Financial and accounting records may be retained after membership ends where required for:

- tax;
- accounting;
- audit;
- contractual evidence;
- fraud prevention;
- or legal claims.



16. Communications and Marketing

KRMA communicates with students, parents, staff and other contacts for both:

- operational purposes; and
- marketing or promotional purposes.

These are not always the same.

16.1 Operational communication

Operational messages may include:

- class changes;
- venue information;
- closures;
- grading arrangements;
- payment administration;
- emergency information;
- policy changes;
- timetable updates;
- collection issues;
- equipment requirements;
- and information necessary to provide the service.

We may send necessary operational communication even where the person has opted out of marketing.

Operational messages should not be used as a disguised way to send unrelated advertising.

16.2 Marketing communication

Marketing may include:

- offers;
- new programmes;

- camps;
- events;
- products;
- newsletters;
- promotions;
- re-engagement campaigns;
- and invitations intended to encourage participation or purchase.

Electronic marketing may be sent through:

- email;
- text message;
- WhatsApp;
- social-media direct message;
- or another electronically stored message.

The Privacy and Electronic Communications Regulations apply to electronic marketing. Marketing to individual subscribers will normally require consent unless a lawful exception, such as the products-and-services soft opt-in, applies and all of its conditions are satisfied.

16.3 Marketing consent

Where we rely upon consent, the person will be given a clear choice.

Consent will not normally be hidden within:

- membership terms;
- general privacy acceptance;
- compulsory forms;
- or pre-ticked boxes.

We will aim to record:

- who consented;
- when;

- communication method;
- information provided at the time;
- and any subsequent withdrawal.

Valid consent requires a genuine choice and a clear positive action.

16.4 Soft opt-in

In some circumstances, KRMA may send marketing concerning similar services to an existing customer without separate consent where:

- the contact details were obtained during a sale or genuine negotiation;
- marketing relates to similar KRMA products or services;
- the person was given a clear opportunity to object when details were collected;
- and every message includes a simple way to opt out.

The soft opt-in does not automatically apply to prospective customers whose details were collected without a qualifying sale or negotiation.

16.5 Social-media marketing

Where KRMA uses social-media advertising, the relevant platform may independently process:

- account information;
- interests;
- device information;
- audience information;
- and interaction data.

KRMA may use:

- general advertising;
- page engagement;
- website visitor audiences;

- or uploaded customer audiences

only where there is an appropriate lawful basis and the use is transparent.

16.6 Opting out

Every person may object to direct marketing.

Marketing messages should provide an easy way to:

- unsubscribe;
- opt out;
- or change preferences.

Opting out of marketing will not normally prevent necessary:

- safety;
- membership;
- payment;
- safeguarding;
- or service communication.

KRMA may retain a limited suppression record to ensure the person is not added back to marketing lists.

16.7 Purchased or third-party lists

KRMA will not assume that a purchased or externally supplied marketing list may be used lawfully.

Before using one, we would need to confirm:

- how information was collected;
- what the person was told;
- what consent or lawful basis exists;
- whether KRMA was identified;
- whether PECR requirements are satisfied;
- and how objections will be honoured.

17. Photographs, Video and Media

KRMA may take or use photographs and recordings to:

- celebrate student achievements;
- document gradings and events;
- promote classes;
- provide educational resources;
- create social-media content;
- support coach development;
- preserve organisational history;
- and provide evidence relating to an incident where appropriate.

Official photographs and videos identifying individuals are likely to constitute personal information and must be handled under data-protection law.

Consent is one possible lawful basis, but the appropriate basis depends upon the purpose and circumstances.

17.1 Promotional media

For identifiable promotional photography involving children, KRMA will normally seek appropriate media permission.

Permission arrangements may identify separate choices for:

- internal use;
- private member communication;
- websites;
- social media;
- printed material;
- press;
- educational resources;
- and external advertising.

Consent for one purpose does not automatically authorise every possible use.

17.2 Student agreement

A child's own wishes will be respected where reasonably possible.

A child who:

- appears distressed;
- asks not to be photographed;
- or does not wish to participate

should not ordinarily be forced into optional promotional media.

17.3 Achievement information

When publishing an achievement, KRMA may use information such as:

- first name;
- age group;
- programme;
- competition result;
- grade;
- or award.

We will aim to avoid unnecessary information that could identify:

- home address;
- school;
- routine;
- medical circumstances;
- or safeguarding arrangements.

17.4 Internal educational recordings

Recordings made for:

- instructor education;
- student feedback;

- technical analysis;
- assessment moderation;
- or private learning

must not automatically be published.

The stated internal purpose, access and retention arrangements will apply.

17.5 Parent and spectator photography

Families taking photographs solely for personal or household use may fall outside organisational data-protection rules.

KRMA may still establish event rules to protect:

- children without media permission;
- privacy;
- safeguarding;
- safety;
- and the smooth running of the activity.

17.6 Restrictions

Photography, recording and livestreaming are not permitted in:

- toilets;
- changing rooms;
- showers;
- personal-care areas;
- bedrooms during residential activities;
- or any area where a person reasonably expects significant privacy.

17.7 Withdrawal of consent

Where we rely upon consent, it may be withdrawn.

Following withdrawal, KRMA will take reasonable steps to stop future use.

It may not always be possible to:

- recall printed materials already distributed;
- remove information lawfully published by independent third parties;
- or undo use that occurred lawfully before withdrawal.

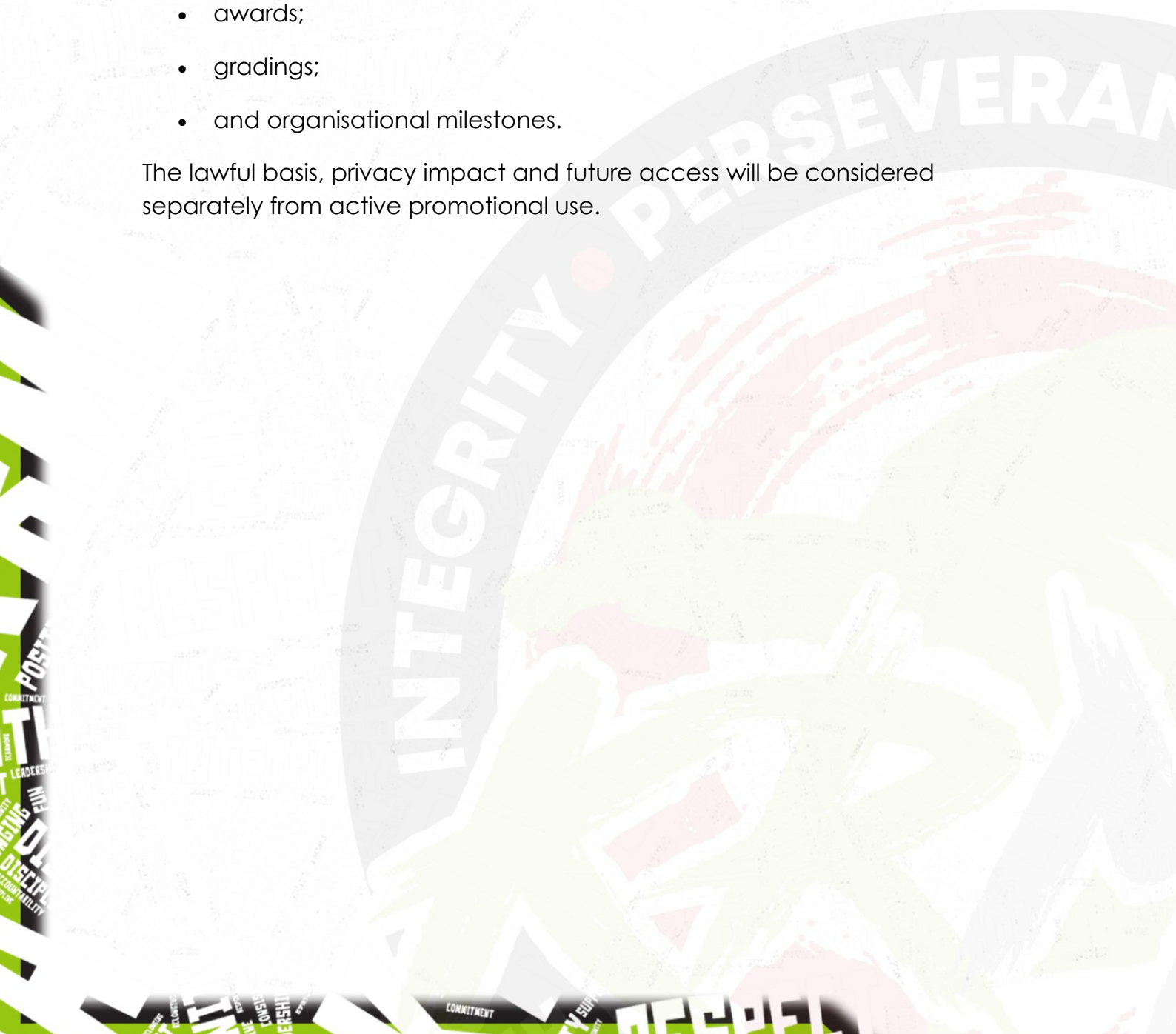
Where practicable, material under KRMA's control will be removed from future campaigns.

17.8 Historic and archive material

KRMA may retain a limited historical archive of significant:

- events;
- teams;
- awards;
- gradings;
- and organisational milestones.

The lawful basis, privacy impact and future access will be considered separately from active promotional use.



18. CCTV and Premises Security

KRMA may use CCTV or similar security systems for purposes including:

- preventing and detecting crime;
- protecting people;
- protecting property;
- investigating incidents;
- safeguarding;
- supporting insurance matters;
- and managing access to premises.

Before using CCTV, KRMA will identify and document an appropriate lawful basis. Surveillance must be necessary, proportionate and transparent.

18.1 CCTV information

CCTV may capture:

- image;
- date;
- time;
- location;
- movement;
- vehicle details;
- and activity within the camera's coverage.

Audio will not normally be recorded.

Audio surveillance is significantly more intrusive and should only be used where necessary, strongly justified and properly assessed.

18.2 Signage and transparency

Where CCTV is in operation, appropriate signs should explain:

- that recording is taking place;

- the purpose;
- the organisation responsible;
- and how further information can be obtained.

The ICO expects CCTV signage to be clear and visible.

18.3 Camera locations

Cameras will not normally be placed within:

- toilets;
- private changing areas;
- showers;
- personal-care spaces;
- or another area where surveillance would be highly intrusive.

Camera angles should avoid unnecessary recording of:

- neighbouring premises;
- private homes;
- unrelated public areas;
- or spaces outside KRMA's legitimate security need.

18.4 Access to footage

CCTV may only be accessed by authorised people for a legitimate purpose.

Footage must not be:

- viewed out of curiosity;
- shown as entertainment;
- posted publicly to shame someone;
- or shared through informal groups.

18.5 Disclosure

Footage may be disclosed where appropriate to:

- police;
- insurers;
- legal advisers;
- venue owners;
- safeguarding agencies;
- people exercising a data right;
- or another organisation with a lawful and proportionate need.

Where footage contains other identifiable people, KRMA may need to:

- redact;
- blur;
- restrict;
- or withhold parts of the recording.

18.6 Retention

Routine footage will be retained for a defined period based upon the security purpose.

Relevant footage may be preserved for longer where connected with:

- an incident;
- safeguarding concern;
- complaint;
- insurance claim;
- police enquiry;
- or legal proceedings.

19. Competitions, Events, Trips and Residential Activities

Participation in external activities may require KRMA to process and share additional information.

This may include:

- name;
- age;
- date of birth;
- grade;
- category;
- weight or height where required;
- contact details;
- emergency contacts;
- medical information;
- disability or support needs;
- media permission;
- transport arrangements;
- dietary requirements;
- accommodation;
- passport information;
- insurance information;
- and payment status.

19.1 Competition organisers

We may share necessary information with:

- competition organisers;
- governing bodies;
- event-registration providers;

- referees or officials;
- medical personnel;
- and category administrators.

Competition organisers may act as independent data controllers and may provide their own Privacy Notice.

19.2 Minimum necessary information

KRMA will aim to share only the information required to:

- enter the participant;
- allocate a safe category;
- deliver the event;
- respond to emergencies;
- and meet legal or insurance requirements.

Routine medical history will not be disclosed where a shorter explanation of the relevant restriction or emergency action is sufficient.

19.3 Travel providers

Information may be shared with:

- coach or transport providers;
- airlines;
- accommodation providers;
- insurers;
- venue operators;
- and activity providers

where necessary to arrange the activity.

19.4 Rooming arrangements

Residential accommodation information may include:

- room allocation;

- age;
- support requirements;
- accessibility;
- safeguarding arrangements;
- and relevant personal preferences.

Rooming information will be limited to people who need it for:

- safeguarding;
- supervision;
- accommodation;
- or administration.

19.5 Passports and identity documents

Passport or identity information will only be collected where genuinely required.

Copies will not be retained longer than necessary for:

- booking;
- travel;
- insurance;
- verification;
- or another lawful purpose.

19.6 Emergency communication

During an emergency or significant disruption, KRMA may share information with:

- parents or carers;
- police;
- medical services;
- travel providers;

- consular authorities;
- insurers;
- event organisers;
- or accommodation staff.

19.7 Photographs and results

Competition and event results may be published by:

- KRMA;
- organisers;
- governing bodies;
- photographers;
- livestream providers;
- or news organisations.

Where another organisation independently determines how results or images are used, its own privacy arrangements will apply.



20. Websites, Cookies and Online Services

When someone visits or uses a KRMA website, we may process:

- IP address;
- browser;
- device type;
- approximate location;
- pages viewed;
- referral source;
- form submissions;
- account information;
- and cookie or similar technology data.

20.1 Website purposes

We may use this information to:

- provide the website;
- maintain security;
- prevent fraud;
- remember preferences;
- understand website performance;
- respond to enquiries;
- improve content;
- manage bookings;
- and measure marketing where permitted.

20.2 Cookies and similar technologies

Websites must provide clear information about cookies and similar technologies.

Consent will be requested before using storage or access technologies where consent is legally required.

Technologies falling within an applicable statutory exception, including those genuinely necessary to provide a service requested by the user, may not require consent. Non-essential technologies must not be treated as necessary merely because they are commercially useful.

20.3 Cookie choices

Where consent is required:

- optional technologies should not be activated before consent;
- the purpose should be explained;
- accepting must involve a positive choice;
- rejecting should be reasonably straightforward;
- and consent should be capable of withdrawal.

Consent cannot be established merely by hiding cookie information within a general Privacy Notice.

20.4 Analytics

KRMA may use analytics to understand:

- visitor numbers;
- page use;
- traffic sources;
- device types;
- and website performance.

The lawful and consent requirements will depend upon:

- the technology;
- information collected;
- provider;
- purpose;

- and whether a statutory exception applies.

20.5 Online forms

Information submitted through an online form will be used for the stated purpose, such as:

- enquiry;
- registration;
- trial booking;
- competition entry;
- consent;
- feedback;
- or recruitment.

Forms should not request more information than is reasonably necessary.

20.6 Links to other websites

KRMA websites may link to:

- payment providers;
- competition organisers;
- governing bodies;
- social-media services;
- retailers;
- or partner organisations.

Once a person follows an external link, the other organisation's privacy and cookie arrangements may apply.

20.7 Children's online services

Where an online service is likely to be used by children, KRMA will consider:

- child-friendly privacy information;
- privacy-protective defaults;

- parental involvement where appropriate;
- profiling;
- direct messaging;
- behavioural tracking;
- unnecessary location information;
- and the child's best interests.



21. Staff, Volunteers, Contractors and Applicants

KRMA processes information concerning people who:

- apply to work or volunteer;
- are employed;
- provide contracted services;
- undertake work experience;
- act as junior instructors;
- or hold another position of responsibility.

A separate recruitment, staff or volunteer Privacy Notice may provide additional detail.

The ICO provides dedicated guidance for employers handling applicant and worker information and recommends clear privacy information for staff and volunteers.

21.1 Recruitment information

We may process:

- application forms;
- CVs;
- employment and volunteering history;
- qualifications;
- martial arts grades;
- references;
- interview notes;
- practical assessments;
- identity;
- right-to-work information;
- DBS information;
- overseas checks;

- driving information;
- and suitability assessments.

We use this to:

- assess applications;
- conduct safer recruitment;
- verify identity and qualifications;
- meet legal responsibilities;
- make appointment decisions;
- and defend or respond to recruitment complaints.

21.2 Staff and volunteer administration

During a role, we may process:

- contact details;
- emergency contacts;
- contracts;
- working hours;
- pay;
- expenses;
- attendance;
- absence;
- health information;
- reasonable adjustments;
- qualifications;
- training;
- appraisal;
- supervision;

- complaints;
- conduct;
- safeguarding concerns;
- and disciplinary information.

21.3 Monitoring and access

Where KRMA monitors:

- system use;
- account access;
- email security;
- CCTV;
- or work performance,

the monitoring must be:

- lawful;
- transparent;
- necessary;
- proportionate;
- and restricted to legitimate purposes.

21.4 Junior instructors

Junior instructors remain children for safeguarding purposes.

Their information may include:

- parental consent;
- training;
- supervision;
- leadership progress;
- emergency information;

- and permitted duties.

They will not be given unnecessary access to confidential staff or student information.

21.5 References supplied by KRMA

Where KRMA provides a reference, it will aim to ensure that the information is:

- accurate;
- fair;
- relevant;
- and provided to an appropriate recipient.

Safeguarding or legal responsibilities may require KRMA to disclose relevant information rather than provide only a general character reference.

21.6 Leaving KRMA

Following departure, information may be retained for:

- employment obligations;
- safeguarding;
- references;
- pensions or payroll where relevant;
- insurance;
- legal claims;
- and verification of qualifications or service.

Access to systems and confidential information will be removed when no longer required.

22. Who We May Share Information With

Depending upon the purpose, KRMA may share personal information with:

- the individual;
- parents or carers;
- authorised collectors;
- emergency contacts;
- instructors and staff;
- payment providers;
- banks;
- accountants;
- insurers;
- legal advisers;
- CRM and software providers;
- email and communication providers;
- website and hosting providers;
- competition organisers;
- governing or membership bodies;
- schools;
- local authorities;
- police;
- healthcare professionals;
- emergency services;
- safeguarding agencies;
- venues;
- transport providers;

- accommodation providers;
- photographers;
- media providers;
- employers or referees;
- courts;
- regulators;
- and other organisations where a lawful reason exists.

In each case, we will aim to consider:

- the purpose;
- lawful basis;
- information required;
- sensitivity;
- security;
- and whether the individual should be informed.

22.1 Independent data controllers

Some recipients determine their own purposes and means of processing.

These may include:

- banks;
- payment providers;
- insurers;
- professional advisers;
- police;
- local authorities;
- competition organisers;
- governing bodies;

- and healthcare providers.

Their own Privacy Notices may apply.

22.2 Identity checks

Before disclosing personal information, we may verify:

- identity;
- authority;
- parental responsibility;
- professional role;
- or legal power.

Being a family member or emergency contact does not automatically provide authority to receive every record.

22.3 Sharing with schools and community partners

Where KRMA delivers a programme with a school or community organisation, information may be shared to:

- administer participation;
- manage safety;
- support inclusion;
- respond to safeguarding concerns;
- assess outcomes;
- or fulfil the agreed service.

The respective roles of KRMA and the partner should be established before regular sharing begins.

22.4 Business or organisational change

If KRMA restructures, transfers part of its operation or changes legal entity, relevant information may be disclosed to:

- advisers;
- insurers;

- funders;
- prospective successor organisations;
- or contractual parties

where lawful and subject to appropriate confidentiality and security.



23. Safeguarding, Emergency and Legal Disclosures

KRMA may disclose personal information without consent where necessary to:

- protect a child;
- protect an adult at risk;
- prevent serious harm;
- respond to an emergency;
- report suspected crime;
- comply with law;
- respond to a court order;
- cooperate with a regulator;
- or establish, exercise or defend legal claims.

23.1 Safeguarding recipients

Safeguarding information may be shared with:

- children's social care;
- adult social care;
- police;
- Local Authority Designated Officer;
- schools;
- healthcare professionals;
- safeguarding partnerships;
- governing bodies;
- insurers;
- and another provider responsible for protecting the person.

23.2 Necessary and proportionate sharing

We will aim to share:

- relevant facts;
- appropriate context;
- necessary identifying details;
- and information required to manage the risk.

We will avoid disclosing unrelated private information.

23.3 Recording the decision

Where practicable, KRMA will record:

- what was shared;
- who received it;
- date;
- purpose;
- lawful basis;
- person making the decision;
- and why consent was or was not obtained.

23.4 Police and authority requests

Before responding to a non-emergency request, KRMA may seek:

- written confirmation;
- the requesting officer's identity;
- statutory authority;
- purpose;
- and scope of information required.

This verification may not be appropriate where delay would create immediate danger.

23.5 Legal proceedings

Relevant information may be preserved or disclosed in connection with:

- court proceedings;

- threatened claims;
- insurance claims;
- employment disputes;
- contractual disputes;
- safeguarding hearings;
- or regulatory investigations.



24. Service Providers and Data Processors

KRMA uses external suppliers to support activities such as:

- membership management;
- CRM;
- attendance;
- payments;
- accounting;
- website hosting;
- email;
- messaging;
- cloud storage;
- forms;
- bookings;
- marketing;
- video;
- and technical support.

Where a supplier handles personal information solely on KRMA's instructions, it acts as a data processor.

24.1 Supplier selection

Before appointing a processor, KRMA will consider matters such as:

- information involved;
- security;
- reliability;
- access controls;
- hosting;
- international transfers;

- subprocessors;
- breach response;
- retention;
- deletion;
- and support for individual data rights.

Controllers must only use processors that provide sufficient guarantees that appropriate technical and organisational protections will be implemented.

24.2 Contracts

A written contract or other binding legal arrangement must normally govern the processing relationship.

The contract should require the processor to:

- act on documented instructions;
- maintain confidentiality;
- apply suitable security;
- control subprocessors;
- assist with data-rights requests;
- assist with breaches and impact assessments;
- return or delete information at the end of the arrangement;
- and provide compliance information where required.

These are core Article 28 requirements for controller–processor relationships.

24.3 Subprocessors

A supplier may use other organisations to provide:

- hosting;
- communications;
- support;
- security;

- or analytics.

KRMA will seek to understand:

- who relevant subprocessors are;
- where they operate;
- what information they receive;
- and what protections apply.

24.4 Supplier security incidents

A processor must notify KRMA without undue delay where it becomes aware of a personal data breach affecting KRMA information.

KRMA remains responsible for assessing whether:

- the ICO;
- affected people;
- insurers;
- safeguarding agencies;
- or another authority

must be notified.

24.5 Ending a supplier arrangement

When a supplier relationship ends, KRMA will seek to ensure that:

- required information is returned or migrated;
- unnecessary information is deleted;
- user access is removed;
- integrations are disconnected;
- and continuing confidentiality obligations are respected.

25. International Transfers

Some of the organisations and technology providers used by KRMA may process or access personal information outside the United Kingdom.

An international transfer may occur where information is:

- stored on servers outside the UK;
- accessed by technical-support staff overseas;
- sent to an overseas competition or event organiser;
- provided to an airline or accommodation provider;
- processed by an international social-media platform;
- or made available to a supplier or subprocessor based outside the UK.

25.1 Transfer protections

Before making a restricted international transfer, KRMA will seek to confirm that an appropriate legal mechanism applies.

This may include:

- UK adequacy regulations;
- the UK International Data Transfer Agreement;
- the UK Addendum to approved standard contractual clauses;
- another approved transfer mechanism;
- or a limited statutory exception that genuinely applies.

Where required, KRMA will also consider whether the destination's laws and practices provide sufficiently effective protection and whether additional technical or contractual safeguards are needed. The ICO updated its international-transfer guidance in January 2026 and provides checklists for identifying and managing restricted transfers.

25.2 Possible additional safeguards

Safeguards may include:

- encryption;
- pseudonymisation;

- restricted user access;
- reduced information fields;
- contractual confidentiality;
- secure transfer systems;
- supplier due diligence;
- and limits upon overseas support access.

25.3 Overseas competitions and trips

Where a student attends an overseas event, KRMA may need to provide information to:

- competition organisers;
- airlines;
- border authorities;
- accommodation providers;
- insurers;
- transport providers;
- medical providers;
- or event partners.

Only information reasonably necessary for the activity should be shared.

This may include:

- name;
- date of birth;
- passport information;
- travel arrangements;
- emergency contact information;
- relevant medical information;
- and competition details.

25.4 Social-media platforms

Material posted through an international social-media service may be processed in several countries under that platform's own arrangements.

Before submitting photographs, testimonials or personal information to social media, individuals should understand that:

- copies may be made;
- content may be shared by others;
- information may remain accessible outside KRMA's direct control;
- and the platform's own Privacy Notice will apply.

KRMA will take reasonable steps to remove material under its control following a valid request, but it may not be able to remove copies independently shared or retained by others.

25.5 Further information

Individuals may contact the Data Protection Lead for further information concerning:

- a particular international transfer;
- the recipient;
- the transfer mechanism;
- and how to obtain information about relevant safeguards.

26. How We Protect Personal Information

KRMA uses proportionate technical and organisational measures to protect personal information from:

- unauthorised access;
- accidental loss;
- theft;
- alteration;
- inappropriate disclosure;
- destruction;
- and loss of availability.

The protection applied will depend upon:

- the type of information;
- its sensitivity;
- number of people affected;
- method of processing;
- likelihood of harm;
- and technology involved.

26.1 Access controls

Access to KRMA systems should be limited according to role.

This may include:

- individual user accounts;
- role-based permissions;
- administrator controls;
- multifactor authentication where available;
- periodic access reviews;
- and prompt removal of access when a person leaves or changes role.

The ability to access a record does not authorise a person to view it without a legitimate work-related reason.

26.2 Password and account security

Staff, instructors and volunteers must:

- use strong and unique passwords;
- protect login information;
- avoid sharing accounts;
- report suspected compromise;
- and follow KRMA security instructions.

Passwords must not be:

- displayed openly;
- sent through insecure messages;
- shared with unauthorised people;
- or reused across personal and KRMA accounts.

26.3 Devices

Devices used to access KRMA information should have suitable protections, which may include:

- automatic screen locking;
- device passwords;
- current software updates;
- encryption;
- malware protection;
- secure configuration;
- and remote-locking or deletion functions where available.

Lost or stolen devices must be reported immediately.

26.4 Secure storage

Electronic records may be stored within:

- approved CRM systems;
- secure cloud storage;
- access-controlled accounts;
- encrypted devices;
- and approved administrative platforms.

Paper records may be stored within:

- locked cabinets;
- controlled offices;
- secure archive storage;
- or another restricted location.

Particularly sensitive information, including:

- safeguarding;
- medical information;
- DBS information;
- criminal allegations;
- financial details;
- and staff disciplinary records

will receive additional access restrictions.

26.5 Email and messaging

Before sending personal information, staff should verify:

- the recipient;
- attachment;
- copied recipients;
- sensitivity;

- and whether a more secure method is required.

Where an email is sent to several unrelated recipients, BCC should normally be used unless recipients have agreed that their addresses may be visible.

Confidential matters must not normally be discussed through:

- unofficial parent groups;
- personal social-media accounts;
- public comments;
- or disappearing-message services.

26.6 Personal devices

Staff should not store confidential KRMA information on personal devices unless:

- the use has been authorised;
- it is operationally necessary;
- suitable protection is present;
- and the information can be securely removed.

Safeguarding, DBS and detailed medical records must not ordinarily be stored locally on personal devices.

26.7 Staff confidentiality

People with access to KRMA information must maintain confidentiality during and after their:

- employment;
- volunteering;
- training;
- contract;
- placement;
- or other appointment.

Leaving KRMA does not permit a person to:

- retain membership lists;
- retain photographs;
- keep private messages;
- use contact details for another organisation;
- or disclose confidential information.

26.8 Supplier security

Suppliers processing information for KRMA will be expected to provide appropriate assurances concerning:

- confidentiality;
- access control;
- system security;
- breach notification;
- data deletion;
- subprocessors;
- and international transfers.

No security measure can eliminate every risk, but KRMA will review and improve controls where:

- systems change;
- risks increase;
- incidents occur;
- or weaknesses are identified.

27. How Long We Retain Personal Information

KRMA retains personal information only for as long as it is reasonably required for:

- the purpose for which it was collected;
- safeguarding;
- contractual responsibilities;
- legal obligations;
- financial records;
- insurance;
- complaints;
- legal claims;
- and organisational accountability.

The law does not establish one universal retention period for every type of personal information. Retention must be justified according to the purpose and circumstances.

KRMA maintains, or will maintain, a more detailed internal Data Retention Schedule.

27.1 Typical retention approach

The following provides an overview of KRMA's normal approach. A record may be retained for a shorter or longer period where the circumstances justify it.

Enquiries and trial bookings

Routine enquiry and trial information will normally be retained for a limited follow-up and administrative period.

It may be retained longer where:

- the person asks to remain in contact;
- marketing consent exists;
- a complaint has arisen;

- or the information is needed for a legal or safeguarding reason.

Membership records

Core membership and contractual information may normally be retained for up to six years after membership ends.

This may include:

- membership agreement;
- payment history;
- significant correspondence;
- and evidence of services provided.

Routine duplicate information may be deleted sooner.

Attendance and progress information

Routine attendance and progress records may be retained during membership and for an appropriate period afterwards to:

- support progression;
- respond to questions;
- maintain programme continuity;
- and manage complaints or claims.

Grading and qualifications

A limited record of formal grades or qualifications may be retained permanently or for the operational life of KRMA.

This may include:

- student name;
- discipline;
- grade;
- date awarded;
- examiner;
- and certificate reference.

Detailed scoring records may be retained for a shorter period.

Financial and accounting records

Financial records will normally be retained for the period required for:

- taxation;
- accounting;
- audit;
- contractual evidence;
- and fraud prevention.

This will commonly be at least six years from the relevant accounting period.

Medical and adjustment information

Current medical and adjustment information will be retained while needed for safe participation.

Information that is no longer current may be:

- updated;
- archived;
- restricted;
- or deleted.

Medical information connected with an accident, safeguarding concern, complaint or legal matter may be retained for longer.

Accident and incident records

Accident, injury and emergency records may be retained according to:

- the age of the person;
- seriousness of the incident;
- health and safety requirements;
- insurance;
- and possible legal claims.

Records involving children may need to be retained beyond the child's eighteenth birthday.

Safeguarding information

Safeguarding records may be retained for a significantly longer period than ordinary membership records.

The period will depend upon:

- the person's age;
- nature of the concern;
- statutory-agency involvement;
- allegation history;
- potential future patterns;
- insurance;
- and safeguarding advice.

Safeguarding records will not be automatically deleted merely because the person leaves KRMA.

Photographs and video

Promotional media will be reviewed periodically and removed where it is:

- outdated;
- no longer necessary;
- no longer appropriate;
- or subject to a valid withdrawal of consent.

Important historical material may be retained separately as part of KRMA's organisational archive where lawful and proportionate.

CCTV

Routine CCTV footage will normally be retained only for a relatively short period.

Footage may be preserved for longer where it relates to:

- crime;
- safeguarding;
- accident;
- complaint;
- insurance;
- disciplinary proceedings;
- or legal action.

Marketing records

Active marketing information may be retained until:

- consent is withdrawn;
- the person objects;
- information becomes inactive;
- or KRMA's periodic review determines that continued use is no longer justified.

A limited suppression record may be retained to ensure that an opt-out is respected.

Recruitment records

Information concerning unsuccessful applicants will normally be retained for a limited period after the recruitment process, commonly around six months, unless:

- the applicant agrees to a longer talent-pool period;
- a complaint or legal matter exists;
- or another legitimate reason applies.

Staff and volunteer information

Personnel records may be retained during the role and for an appropriate period afterwards to meet:

- employment;

- safeguarding;
- tax;
- pension;
- insurance;
- reference;
- and legal-claim requirements.

Some safeguarding and suitability information may require longer retention.

27.2 Retention holds

Normal deletion may be suspended where information is relevant to:

- a safeguarding concern;
- data-rights request;
- complaint;
- disciplinary process;
- police investigation;
- insurance matter;
- legal claim;
- or regulatory enquiry.

Information should not be destroyed to prevent disclosure or avoid accountability.

27.3 Secure disposal

When information is no longer required, KRMA will seek to:

- delete it securely;
- destroy confidential paper;
- remove unnecessary copies;
- instruct suppliers to delete or return it;
- or anonymise it where continued statistical use is appropriate.

28. Your Data-Protection Rights

Individuals have rights relating to their personal information.

The available right and outcome will depend upon:

- why the information is used;
- lawful basis;
- type of information;
- safeguarding;
- legal obligations;
- and the rights of other people.

The principal rights include the following.

28.1 Right to be informed

You have the right to receive clear information about:

- what KRMA collects;
- why it is collected;
- how it is used;
- who it is shared with;
- how long it is retained;
- and what rights you have.

This Privacy Notice is one way in which KRMA provides that information.

28.2 Right of access

You may ask KRMA to confirm whether we use your personal information and request:

- a copy of that information;
- information about its purposes;
- recipients;
- retention;

- and other relevant processing details.

This is commonly known as a **subject access request**.

The request does not need to use a particular form or legal wording.

28.3 Right to rectification

You may ask KRMA to correct inaccurate personal information or complete information that is materially incomplete.

Where a record correctly describes:

- an allegation;
- observation;
- opinion;
- or decision made at a particular time,

disagreement does not necessarily make the record inaccurate.

KRMA may record the disagreement or add an explanatory note where appropriate.

28.4 Right to erasure

You may ask KRMA to delete personal information in certain circumstances.

This right is not absolute.

Information may need to be retained for:

- safeguarding;
- legal obligations;
- legal claims;
- financial records;
- contractual evidence;
- or another lawful reason.

Where deletion cannot be completed, KRMA will explain why.

28.5 Right to restrict processing

You may ask KRMA to restrict how information is used while:

- accuracy is considered;
- an objection is assessed;
- processing is disputed;
- or information is required for a legal claim.

Restricted information will normally be stored but not otherwise used except where the law permits.

28.6 Right to object

You may object to processing based upon:

- legitimate interests;
- public task;
- or direct marketing.

An objection to direct marketing will be honoured.

Where another objection is made, KRMA will assess whether compelling lawful reasons justify continuing the processing.

28.7 Right to data portability

In certain circumstances, you may request information you provided to KRMA in a:

- structured;
- commonly used;
- and machine-readable format.

This right generally applies where processing:

- is automated;
- is based upon consent or contract;
- and concerns information supplied by the person.

28.8 Right to withdraw consent

Where KRMA relies upon consent, you may withdraw it at any time.

Withdrawal does not make earlier lawful processing unlawful.

It may also not require deletion where another legal reason requires KRMA to keep the information.

28.9 Rights concerning automated decisions

You may have rights where a significant decision is made about you solely through automated processing without meaningful human involvement.

Further information appears in Section 31.

28.10 Making a request

Requests may be sent to:

Email: admin@krma.co.uk

Telephone: 01652 653560

or by post to:

Koku-Ryu Martial Arts

Unit 22 Island Carr Road
Brigg
North Lincolnshire
DN20 8PD

Please mark the request:

For the attention of the Data Protection Lead

28.11 Identity verification

KRMA may ask for proportionate information to confirm:

- identity;
- authority;
- or the person on whose behalf the request is being made.

This is intended to prevent personal information being disclosed to the wrong person.

28.12 Response period

KRMA will normally respond to a valid data-rights request without undue delay and within one month.

Where a request is complex or several requests are made, the response period may be extended by up to a further two months where legally permitted. The person must be informed of the extension and reason within the initial period.

28.13 Charges

Requests will normally be handled without charge.

A reasonable fee may be considered only where the law permits, including where a request is manifestly unfounded or excessive or where additional copies are requested.

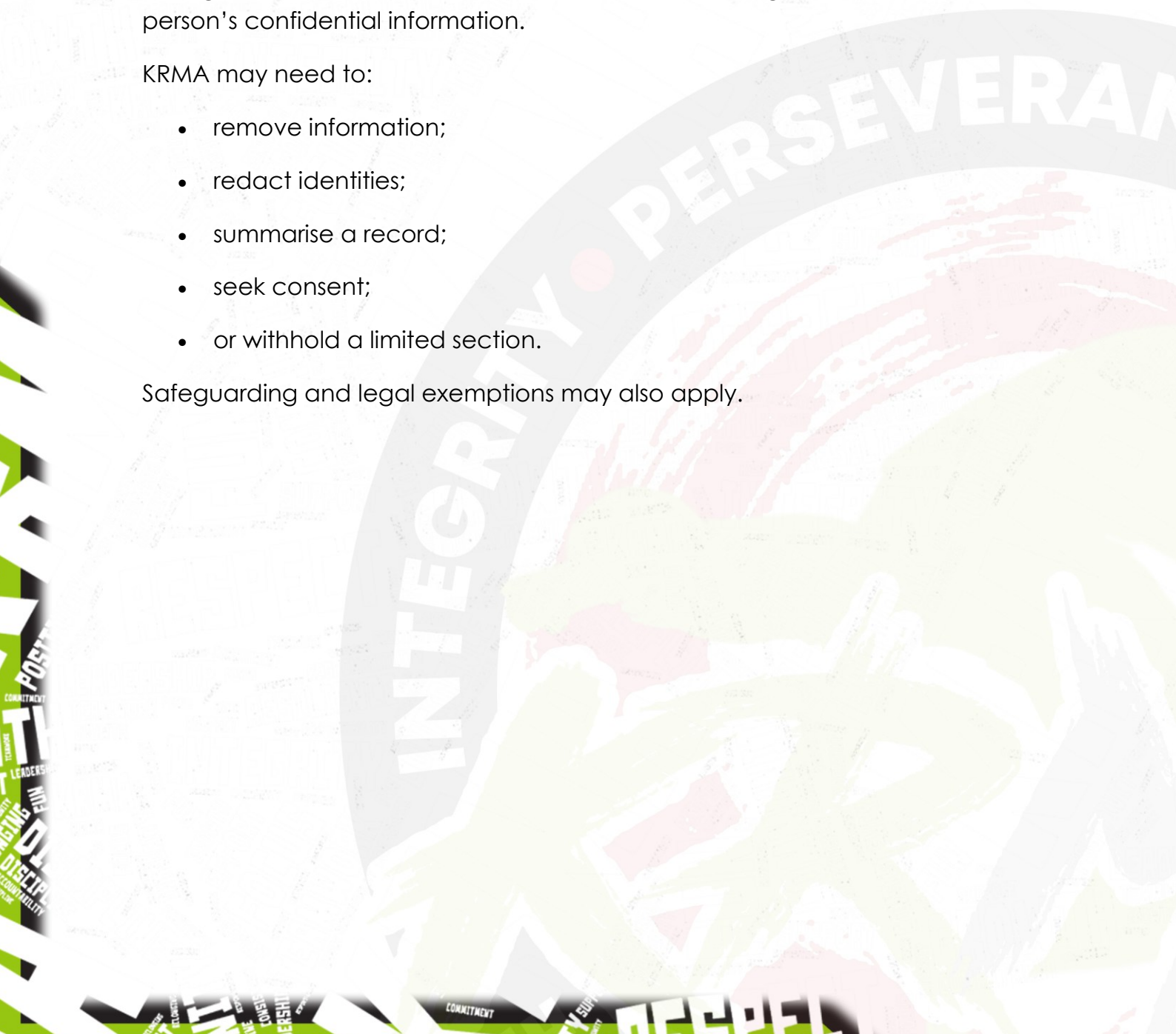
28.14 Information concerning other people

The right of access does not automatically provide a right to receive another person's confidential information.

KRMA may need to:

- remove information;
- redact identities;
- summarise a record;
- seek consent;
- or withhold a limited section.

Safeguarding and legal exemptions may also apply.



29. Children's Rights and Requests Made by Parents or Carers

Data-protection rights belong to the child.

A parent or carer may exercise a child's rights where:

- the child authorises them;
- the child does not have sufficient understanding to act independently;
- the request is lawfully made on the child's behalf;
- or another legal authority applies.

A child who is sufficiently competent to understand the request may exercise their own data-protection rights. The ICO's guidance requires organisations to assess the individual child's understanding rather than relying solely upon age.

29.1 Factors considered

KRMA may consider:

- age;
- maturity;
- ability to understand;
- nature of the information;
- consequences of disclosure;
- child's wishes;
- parental responsibility;
- family circumstances;
- safeguarding concerns;
- and court orders.

29.2 Parental responsibility

Before disclosing a child's information to an adult, KRMA may ask for evidence of:

- identity;

- parental responsibility;
- legal authority;
- or the child's permission.

Being named as:

- emergency contact;
- authorised collector;
- grandparent;
- family friend;
- or partner of a parent

does not automatically provide the right to access all of a child's records.

29.3 Separated families

KRMA will remain neutral in disputes between parents or carers.

A request from one parent must not automatically result in disclosure of:

- the other parent's confidential contact details;
- private correspondence;
- court-protected information;
- safeguarding reports;
- or information concerning another person.

29.4 Safeguarding restrictions

KRMA may restrict or refuse disclosure where providing the information could:

- place the child at risk;
- identify a confidential source;
- compromise a police or social-care enquiry;
- expose another child's information;
- or conflict with a legal restriction.

The decision will be considered carefully with the Data Protection Lead and, where relevant, the Designated Safeguarding Lead.

29.5 Child-friendly responses

Where a response is provided directly to a child, KRMA will aim to make it:

- clear;
- age-appropriate;
- accessible;
- and understandable.



30. Withdrawing Consent

Where KRMA relies upon consent, consent may be withdrawn at any time.

Examples may include consent for:

- optional marketing;
- promotional photography;
- testimonials;
- selected video use;
- and other genuinely optional processing.

30.1 How to withdraw consent

A request may be made through:

- email;
- telephone;
- written communication;
- approved preference settings;
- unsubscribe link;
- or direct communication with an authorised member of staff.

Requests should identify:

- the person;
- processing involved;
- and consent being withdrawn.

30.2 Effect of withdrawal

Following withdrawal, KRMA will:

- record the request;
- stop future processing based solely upon that consent;
- update relevant systems;

- inform processors where necessary;
- and remove material under KRMA's control where reasonably practicable.

30.3 Existing publications

Withdrawal may not make it possible to:

- recall printed material already distributed;
- remove independent press coverage;
- retrieve copies shared by other people;
- or reverse processing that occurred lawfully before withdrawal.

KRMA will nevertheless stop using the material in future campaigns where consent was the only lawful basis.

30.4 Core services

Where information is genuinely required to:

- provide the agreed service;
- protect safety;
- fulfil a legal obligation;
- manage safeguarding;
- or respond to an emergency,

KRMA may rely upon a lawful basis other than consent.

Withdrawal of optional consent does not automatically require KRMA to stop necessary operational processing.

31. Automated Processing and Artificial Intelligence

KRMA may use technology or artificial intelligence to support activities such as:

- drafting routine communication;
- organising information;
- analysing anonymised trends;
- scheduling;
- administrative assistance;
- and producing marketing concepts.

KRMA will not allow an AI system to make an unreviewed final decision concerning:

- safeguarding;
- membership termination;
- disciplinary action;
- grading;
- staff suitability;
- scholarship awards;
- complaints;
- reasonable adjustments;
- or access to essential services.

31.1 Human responsibility

Where AI supports a task, an authorised person remains responsible for:

- checking accuracy;
- considering context;
- identifying bias;
- correcting mistakes;

- protecting confidentiality;
- and making the final decision.

31.2 Information entered into AI systems

KRMA staff must not place identifiable:

- safeguarding records;
- DBS information;
- detailed medical information;
- criminal allegations;
- confidential complaints;
- passwords;
- payment information;
- identity documents;
- or private information about children

into an unapproved public AI system.

31.3 Significant automated decisions

Data-protection law permits significant automated decisions in a wider range of circumstances than previously, provided a valid lawful basis and appropriate safeguards apply. Special category information remains subject to stronger restrictions. Relevant safeguards may include meaningful human involvement, reconsideration and an opportunity for the person to make representations.

31.4 Notification

Where KRMA introduces processing involving a significant solely automated decision, we will provide appropriate information concerning:

- the use of automation;
- relevant logic or factors;
- possible consequences;
- human review;

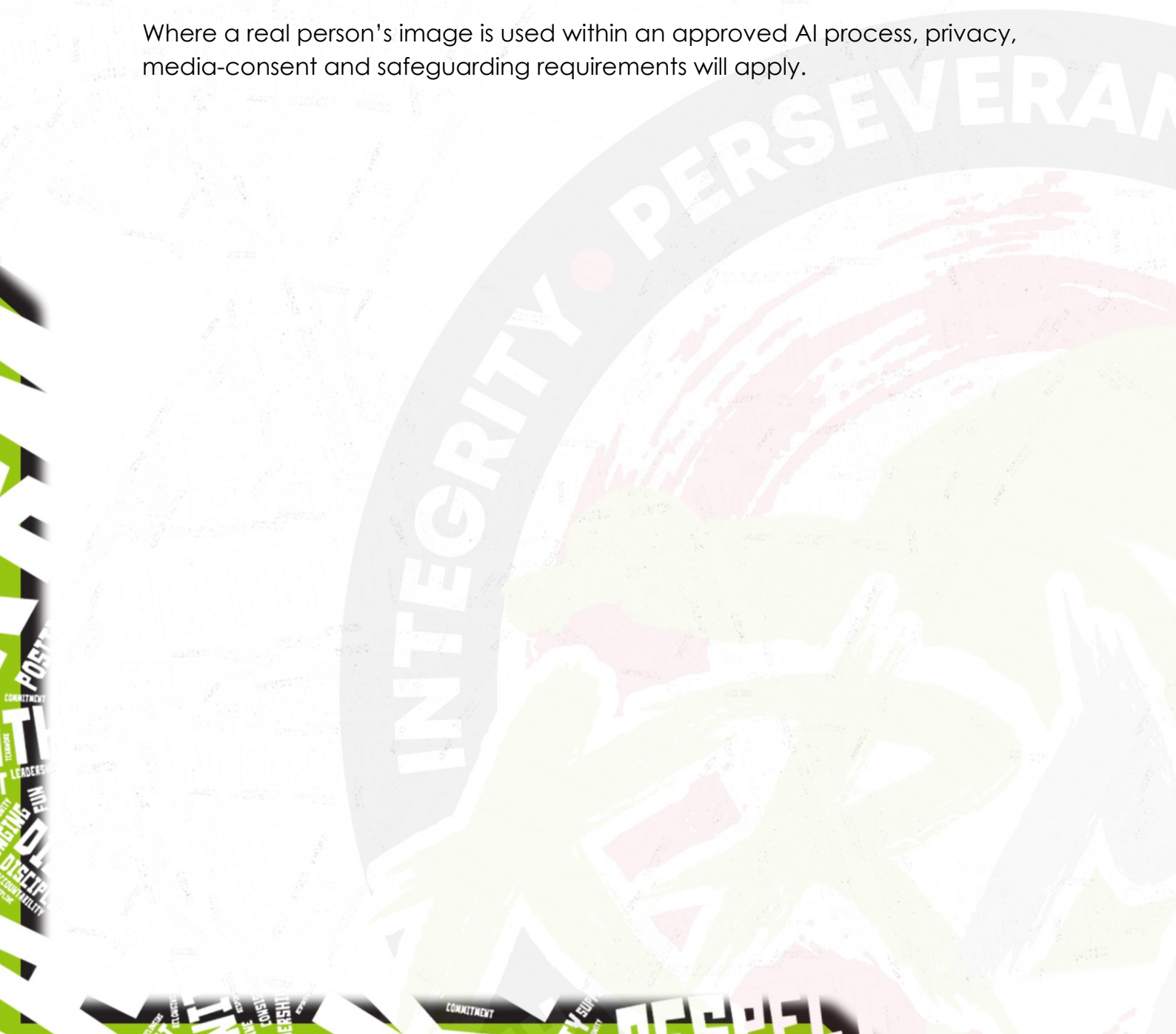
- and how the decision may be challenged.

31.5 AI-generated images and content

KRMA will not knowingly use AI to create:

- misleading images of students;
- fabricated achievements;
- false safeguarding evidence;
- harmful impersonation;
- sexualised material;
- or content intended to humiliate someone.

Where a real person's image is used within an approved AI process, privacy, media-consent and safeguarding requirements will apply.



32. Personal Data Breaches

A personal data breach is a security incident that results in personal information being:

- lost;
- destroyed;
- altered;
- disclosed;
- accessed;
- or made unavailable

accidentally or unlawfully.

Examples may include:

- sending an email to the wrong person;
- losing a device;
- unauthorised CRM access;
- account compromise;
- stolen paper records;
- public disclosure of confidential information;
- lost safeguarding records;
- unauthorised photographs;
- ransomware;
- or accidental deletion.

32.1 KRMA's response

Where a breach is identified, KRMA will seek to:

1. Contain the incident.
2. Protect affected people.
3. Preserve relevant evidence.

4. Recover information where possible.
5. Assess the likely risks.
6. Decide whether notification is required.
7. Document the incident.
8. Take action to prevent recurrence.

32.2 ICO notification

Where a breach is likely to result in a risk to people's rights and freedoms, KRMA must report it to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it.

Not every breach must be reported to the ICO, but every confirmed breach should be assessed and recorded.

32.3 Informing affected people

Where a breach is likely to result in a high risk to affected individuals, KRMA will notify them without undue delay unless an applicable legal exception applies.

The communication may explain:

- what happened;
- information involved;
- likely consequences;
- action taken;
- protective steps;
- and who to contact.

32.4 Children and safeguarding

Where a breach affects a child, KRMA will also consider:

- physical safety;
- collection or location risk;
- family circumstances;

- safeguarding agencies;
- whether the child should be informed directly;
- and whether informing a parent could increase danger.



33. Data-Protection Complaints and the Information Commissioner

Anyone who is concerned about KRMA's handling of personal information may raise a data-protection complaint.

The complaint may concern matters such as:

- inaccurate information;
- inappropriate sharing;
- security;
- marketing;
- photography;
- CCTV;
- failure to respond to a request;
- refusal to delete information;
- or another privacy concern.

33.1 Complaining to KRMA

Complaints may be sent to:

Email: admin@krma.co.uk

Telephone: 01652 653560

or by post to:

Koku-Ryu Martial Arts

Unit 22 Island Carr Road
Brigg
North Lincolnshire
DN20 8PD

Please mark the complaint:

For the attention of the Data Protection Lead

33.2 Information to include

It is helpful to provide:

- name;

- contact details;
- nature of the concern;
- relevant dates;
- people involved;
- previous communication;
- and the outcome being requested.

A complaint will not be rejected merely because it does not refer to data-protection law.

33.3 KRMA's response

KRMA will:

- provide a clear way to complain;
- acknowledge the complaint within 30 days;
- investigate without undue delay;
- keep the person appropriately informed;
- and communicate the outcome without unjustifiable delay.

These complaint-handling requirements came into force across the UK in June 2026.

33.4 Possible outcomes

Depending upon the findings, KRMA may:

- correct information;
- remove inappropriate material;
- restrict processing;
- change permissions;
- provide additional information;
- apologise;
- retrain staff;

- change a supplier;
- strengthen security;
- revise a procedure;
- or explain why the processing remains lawful.

33.5 Complaining to the ICO

Individuals also have the right to raise a concern with the Information Commissioner's Office.

The ICO will normally expect the individual to give the organisation an opportunity to address the matter first.

The ICO's public helpline is:

0303 123 1113

Its current head-office address as at the effective date of this Notice is:

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

The ICO has announced that its head office is expected to relocate later in 2026, so its official contact service should be checked before sending post.

Raising a complaint will not result in retaliation or loss of membership merely because the person has questioned KRMA's use of personal information.

34. Changes to This Privacy Notice

KRMA may update this Privacy Notice where:

- legislation changes;
- ICO guidance changes;
- systems change;
- new services are introduced;
- suppliers change;
- international transfers change;
- CCTV or AI is introduced;
- retention arrangements change;
- or our information practices develop.

34.1 Material changes

Where a change is likely to have a significant effect upon individuals, KRMA will take reasonable steps to draw attention to it.

This may include:

- email;
- website notice;
- membership communication;
- staff briefing;
- updated forms;
- or direct contact.

34.2 Previous versions

KRMA may retain previous versions of this Privacy Notice to demonstrate:

- what people were told;
- when the notice applied;
- and how our processing arrangements changed.

34.3 Review cycle

This Privacy Notice will be reviewed:

- at least annually;
- following significant legal change;
- following a serious data breach;
- after major changes to systems;
- following introduction of significant AI or surveillance;
- or whenever a material privacy concern is identified.

Privacy Summary

KRMA may use personal information to:

- provide martial arts programmes;
- manage membership and payments;
- keep students safe;
- support medical and additional needs;
- record progress and achievements;
- organise events and travel;
- communicate with families;
- recruit and manage suitable staff;
- and promote KRMA where appropriate.

We will aim to:

- collect only what we need;
- explain how it is used;
- protect it;
- share it only for legitimate reasons;
- retain it only as long as necessary;

- and respect individual rights.

Questions or requests should be directed to:

Data Protection Lead

Email: admin@krma.co.uk

Telephone: 01652 653560



Document Approval

Document title: Privacy Notice

Organisation: Koku-Ryu Martial Arts

Data controller: Koku-Ryu Martial Arts

Version: 2.0

Document owner: CEO and Chief Instructor

Operational responsibility: Data Protection Lead

Approved by: Andrew Banks – CEO and Chief Instructor

Effective date: 14 July 2026

Next review date: 14 July 2027

Our Commitment

Koku-Ryu Martial Arts recognises that privacy is essential to:

- safeguarding;
- trust;
- dignity;
- fairness;
- and responsible organisational management.

We will not treat personal information as merely an administrative resource.

The information we hold relates to real people, including children, families, staff and volunteers, and must therefore be handled:

- respectfully;
- carefully;
- lawfully;
- and securely.