

Introduction

Croydon Amphibians Swimming Club needs to gather and use certain information about individuals. These include active members, prospective members held on a waiting list, business contacts, employees and other people the Club has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the Club's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Croydon Amphibians Swimming Club:

- Complies with data protection law and follow good practice.
- Protects the rights of Employees, members and others.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Data protection laws

The Data Protection Act 1998 and, from May 2018, the General Data Protection Regulation (GDPR) describes how organisations — including Croydon Amphibians Swimming Club— must collect, handle and store personal information. The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act. They give people specific privacy rights in relation to electronic communications.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act and GDPR are underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully,
2. Be obtained only for specific, lawful purposes,
3. Be adequate, relevant and not excessive,
4. Be accurate and kept up to date,
5. Not be held for any longer than necessary,
6. Be processed in accordance with the rights of data subjects,
7. Be protected in appropriate ways, and
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

The GDPR details the following rights:

1. the right to be informed,
2. the right of access,
3. the right to rectification,
4. the right to erasure,
5. the right to restrict processing,
6. the right to data portability,
7. the right to object, and
8. the right not to be subject to automated decision-making including profiling.

People, risks and responsibilities

Policy scope

This policy applies to:

- Members of the Executive Committee.
- All Employees and volunteers of Croydon Amphibians Swimming Club.
- All contractors, suppliers and other people working on behalf of Croydon Amphibians Swimming Club.

It applies to all data that the Club holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This includes, but is not restricted to:

- Names of individuals.
- Postal addresses.
- Email addresses.
- Telephone numbers.
- Dates of birth.

Legal basis for holding and using data

The GDPR requires each organisation that holds personal data on individuals to define the legal basis on which they hold and use this data.

Croydon Amphibians Swimming Club primarily holds data for Club members and employees and will only use this data for legitimate purposes. The legal activities of the Club are defined in the Club's Constitution, our membership rules and our bye laws. These are publicly available on our website or available by direct request to the Club.

The Club will only hold and use data for the purposes detailed in these documents. Hence the Club's legal basis as allowed by the GDPR is "Legitimate Interest".

The absolute minimum data required for the Club to carry out its membership activities are member names, dates of birth, postal addresses, email addresses and telephone numbers; all of which enable the Club carry out its membership activities efficiently and economically.

The Club also holds other personal data on swim meet guests/competitors, prospective members, volunteers and officials. This data is held for either legal, insurance or for the legitimate activities of the Club as laid out in the Club's Constitution, our membership rules and our bye laws. The Club's legal basis as allowed by the GDPR is again "Legitimate Interest".

Data protection risks

This policy helps to protect Croydon Amphibians Swimming Club from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the Club contacts them for legitimate reasons i.e. membership renewal, Club AGM notification etc.
- Reputational damage. For instance, the Club could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Croydon Amphibians Swimming Club has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Executive Committee is ultimately responsible for ensuring that Croydon Amphibians Swimming Club meets its legal obligations, including:
 - Keeping the Club updated about data protection responsibilities, risks and issues.
 - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
 - Arranging data protection training and advice for the people covered by this policy.
 - Handling data protection questions from employees, members and anyone else covered by this policy.
 - Dealing with requests from individuals to see the data Croydon Amphibians Swimming Club holds about them (also called 'subject access requests').

General employee and volunteer guidelines

- The only people able to access data covered by this policy are those who need it for their work.
- Data must not be shared informally. When access to personal data is required employees can request it from the Executive Committee.
- Croydon Amphibians Swimming Club will provide training to all employees and, when applicable, volunteers to help them understand their responsibilities when handling data.
- Employees and volunteers must keep all data secure, by taking sensible precautions and following the guidelines below.
 - Strong passwords must be used, and they must never be shared.
 - Personal data must not be disclosed to unauthorised people, either within the Club or externally.
 - Data must be regularly reviewed and updated if it is found to be out of date. If no longer required, it must be deleted and disposed of.
 - Employees/volunteers must request help from the Executive Committee if they are unsure about any aspect of data protection.

Data storage

This section describes how and where data must be safely stored. Questions about storing data safely can be directed to the Executive Committee.

When data is stored on paper, it must be kept in a secure place where unauthorised people cannot see it. This includes data that is usually stored electronically but has been printed out:

- When not required, the paper or files must be kept in a locked drawer or filing cabinet.
- Employees/volunteers must make sure paper and printouts are not left where unauthorised people could see them.
- Data on paper must be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data must be protected by strong passwords that are changed regularly and never shared.
- If data is stored on removable media (like a disk or memory card/key), these must be kept locked away securely when not being used.
- Data must only be stored on designated Club laptops, and must only be uploaded to approved cloud computing services.
- Club laptops containing personal data must be kept locked away securely when not being used.
- Data must be backed up frequently. Those backups must be tested regularly, in line with the Club's standard backup procedures.
- Data must never be saved directly to laptops or other mobile devices like tablets or smart phones not belonging to the Club.

Data use

Personal data is of no value to Croydon Amphibians Swimming Club unless the Club can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees and volunteers must ensure the screens of their computers are always locked when left unattended.
- Personal data must not be shared informally. In particular, it must never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The Executive Committee can explain how to do this.
- Personal data must never be transferred outside of the European Economic Area.
- Personal data must always be accessed and update using the central copy of any data.
- Personal data must not be saved on any device other than those owned by the Club.

Data accuracy

The law requires Croydon Amphibians Swimming Club to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Croydon Amphibians Swimming Club must put into ensuring its accuracy.

It is the responsibility of all employees and volunteers who work with personal data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Employees and volunteers must not create any unnecessary additional data sets.
- Employees and volunteers must take every opportunity to ensure data is updated. For instance, by confirming a member's details when they contact the Club.
- Croydon Amphibians Swimming Club will make it easy for data subjects to update the information that the Club holds about them. For instance, via the membership renewal process.
- Data must be updated as inaccuracies when discovered. For instance, if a member can no longer be reached on their stored telephone number or email address, it must be removed from the database.
- Members who unsubscribe from email communication must never be contacted by this method and any email information must be removed from Club records.

Subject access requests

All individuals who are the subject of personal data held by Croydon Amphibians Swimming Club are entitled to:

- Know what information the Club holds about them and why.
- Know how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the Club is meeting its data protection obligations.

If an individual contacts the Club requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email or letter, addressed to the Executive Committee.

The Club will respond to subject access requests free of charge. However, the Club reserves the right to charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee charged will be based on the administrative cost of providing the information.

The Executive Committee will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the data protection legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Croydon Amphibians Swimming Club will disclose requested data. However, the Executive Committee will ensure the request is legitimate, seeking assistance from the Club's Chair and Secretary, and from the Club's legal advisers where necessary.

Personal data breach

If there is an actual or suspected personal data breach this must be reported to the Executive Committee without delay. The Executive Committee will investigate and determine what action is necessary.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Croydon Amphibians Swimming Club will:

- Take action to prevent any further data breaches.
- Inform those people adversely affected without delay.
- Document the data breach and actions taken.
- If appropriate, inform the Information Commissioner's Office within 72 hours.
- If relevant, instigate disciplinary proceedings.

Providing information

Croydon Amphibians Swimming Club aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

To these ends, the Club has a privacy statement setting out how data relating to individuals is used by the Club. This is available on request. A version of this statement is also available on the website.

Electronic Communication

- Email communications will only be used where a person has provided the Club with their email address.
- Having provided an email address and/or telephone number, a member can have those details removed from the Club's records at any time. Individuals are prompted to correct and add or remove details when they join the Club and when they renew their membership.
- For those choosing not to receive emails from the Club, information will be provided on the Club's website, Twitter and notices at the pools (where possible). Membership applications will be sent by post to these individuals.
- Blind copy must be used for member, employee, volunteer group and event participant emails.
- Employees and volunteers must always use a Club email address when communicating on behalf of the Club with external organisations.

Appendix A - Member privacy statement

Croydon Amphibians Swimming Club takes your privacy seriously and we will only use your personal information for legitimate Club purposes, which may include some or all of the following:

- *administer your membership,*
- *keep you informed about Club news, events and fund raising, projects and activities, employment and volunteering opportunities.*

We will not pass your personal information to third parties except when legally required to do so.

We will keep your personal information for 2 years after your membership has lapsed.

Further information regarding our data protection policy can be obtained by contacting the Club directly or from our website.