Data Protection Policy

Document History

Version	Date	Notes
Initial	02/02/2017	Policy written
1	23/02/2017	Policy approved

Introduction

City of Norwich AC (CoNAC/the club) needs to gather and use certain information about individuals.

These can include members, volunteers (which also includes trustees, officials, coaches & team managers), customers, suppliers, 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.

The consequences for breaching relevant data protection and privacy legislation could be serious for CoNAC, members and associates may lose trust in how we manage their data, there may be damage to the CoNAC brand and reputation and enforcement action may be take action against CoNAC.

Why This Policy Exists

This data protection policy ensures City of Norwich Athletic Club

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

Data Protection Law

The Data Protection Act 1998 describes how organisations including CoNAC must collect, handle and store personal information.

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 is 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. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- All volunteers and staff of CoNAC
- All contractors, suppliers and other people working on behalf of CoNAC

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 can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data Protection Risks

This policy helps to protect CoNAC 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 CoNAC uses data relating to them.
- Reputational damage. For instance, CoNAC could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who volunteers or works for or with CoNAC has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person or 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 CoNAC meets its legal obligations.

- The Membership Officer is responsible for:
    - Keeping the executive committee updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Handling data protection questions from volunteers, staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data CoNAC holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle CoNAC's sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Evaluating any third-party services the club is considering using to store or process data. For instance, cloud computing services.

General Volunteer and Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work or club duties.
- Data should not be shared informally. When access to confidential information is required, volunteers and employees can request it from the Membership Officer.
- Volunteers and employees should keep all data secure, by taking sensible precautions and following the guidelines below.
    - In particular, strong passwords must be used and they should never be shared.
    - Personal data should not be disclosed to unauthorised people, either within the club or externally.
    - Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of in a secure way in which the data cannot be read or used by anyone else (for example shredding).
    - Volunteers and employees should request help from the Membership Officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Membership Officer.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Volunteers and employees should make sure paper and printouts are not left where unauthorised people could see them, such as on a printer.
- Data printouts should 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 should be protected by strong passwords that are changed regularly and never shared with anybody else.
- If data is stored on removable media (such as a CD, DVD or Flash Drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently.
- Data should never be saved directly to desktop computers, laptops or other mobile devices such as tablets or smart phones.

Data Use

Personal data is of no value to CoNAC unless they 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, volunteers and employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area unless that country or territory also ensures an adequate level of protection.
- If your role changes and you no longer have the need to access data or you leave CoNAC all data you hold must be destroyed in a secure manner (such as shredding documents) or deleting any locally held data.

Data Accuracy

The law requires CoNAC 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 CoNAC should put into ensuring its accuracy.

It is the responsibility of all volunteers and employees who work with 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. Volunteers and staff should not create any unnecessary additional data sets.
- CoNAC will make it easy for data subjects to update the information it holds about them. For instance, via the membership system.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

All individuals who are the subject of personal data held by CoNAC are entitled to:

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

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

Subject access requests from individuals should be made by email, addressed to the Membership Officer at membership@conac.org.uk.

Individuals will be not be charged for a subject access request. The Membership Officer will aim to provide the relevant data within 14 days.

The Membership Officer 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 Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CoNAC will disclose requested data. However, the Membership Officer will ensure the request is legitimate, seeking assistance from the executive committee and from legal advisers where necessary.

Providing Information

CoNAC 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, CoNAC has a privacy statement, setting out how data relating to individuals is used.

This statement is also available on the CoNAC website.