2019

Privacy Personal Data Protection Policy

NEWPORT COUNTY AFC

Document type	Privacy Personal Data Protection Policy
Drafted by	Ben Jones
Signed off by	Gavin Foxall
Board review and agreement	April 2019
Next review date	April 2020
Version I.D.	1

1. Introduction

In its everyday business operations Newport County AFC makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Newport County AFC is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to or interface with Newport County AFC systems.

The following policies and procedures are relevant to this document:

- *Records Retention and Protection Policy*
- *GDPR Management Intranet*
- *GDPR Intranet Training Module*
- *Information Security Incident Response Procedure*

2. Privacy and Personal Data Protection Policy

The General Data Protection Regulation

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that Newport County AFC carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is Newport County AFC's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

Definitions

There is a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier

such as a name, an identification number, location data, an online identifier or to one or more factor specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'processing' means*:*

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'controller' means*:*

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the GDPR is based. These are as follows:

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairnessand transparency');
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Newport County AFC will ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

3. Rights of the Individual

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the club will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

The data subject also has rights under the GDPR. These consist of:

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
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within Newport County AFC, managed by the GDPR Intranet, that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown in Table 1.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Table 1 - Timescales for data subject requests

4. Lawfulness of Processing

The club and its designated safeguarding officers will act in line with the HM Government guidance, *Information sharing: advice for safeguarding practitioners providing safeguarding services* (Department for Education, March 2015) which describes the following '7 Golden Rules' of information sharing:

1. **Remember that the Data Protection Act 1998 and human rights law are not barriers** to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. **Be open and honest with the individual** (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. **Seek advice from other practitioners** if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. **Share with informed consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk.
5. **Consider safety and well-being**: Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. **Necessary, proportionate, relevant, adequate, accurate, timely and secure**: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
7. **Keep a record of your decision and the reasons for it**– whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Club safeguarding records contain sensitive personal information and are treated as highly confidential. They will not be disclosed except where information sharing is in the interests of protecting a child from significant harm or potential harm as the welfare and protection of children and young people is always the paramount consideration (Children Act 1989).

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. It is Newport County AFC policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described in brief in the following sections.

Consent

Unless it is necessary for a reason allowable in the GDPR, Newport County AFC will always obtain explicit consent from a data subject to collect and process their data. In case of children below the age of 1 parental consent will be obtained. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject, then this information will be provided to the data subject within a reasonable period after the data are obtained and definitely within one month.

Newport County AFC has adopted a preference system, to allow its supporters to access and control their information requirements and preferences directly, in accordance with the requirements and recommendations of the GDPR.

Performance of a Contract

Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g. a delivery cannot be made without an address to deliver to.

Legal Obligation

If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.

Vital Interests of the Data Subject

In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. Newport County AFC will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data.

Task Carried Out in the Public Interest

Where Newport County AFC needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

Legitimate Interests

If the processing of specific personal data is in the legitimate interests of Newport County AFC and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

5. Privacy by Design

Newport County AFC has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data

- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.

6. Contracts Involving the Processing of Personal Data

Newport County AFC will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR.

7. International Transfers of Personal Data

Transfers of personal data outside the European Union will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR.

Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

8. Data Protection Officer

Newport County AFC has appointed a Data Protection Officer to ensure that compliant processes are instigated and to manage ongoing compliance with the GDPR.

The Data Protection Officer may be contacted via the Club's main telephone number or by email at DPO@reddrum.co.uk

9. Breach Notification

It is Newport County AFC's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents, by the Club's GDPR Intranet Management System.

10. Addressing Compliance to the GDPR

The GDPR contains provisions intended to enhance the protection of children's personal data and to ensure that children are addressed in plain, clear language that they can understand. Transparency and accountability are important where children's data is concerned, and this is especially relevant when they are accessing online services. However, in all circumstances the Club will carefully consider the level of protection that we are giving that data.

Recital 38 of the GDPR states that:

"Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

NCAFC believes that transparency is key. The Club will seek to raise children's (and their parents') awareness of data protection risks, consequences, safeguards and rights by:

- telling them what we are doing with their personal data;
- being open about the risks and safeguards involved; and
- letting them know what to do if they are unhappy.

Under no circumstances will the club disclose personal information or data without written and fully informed consent:

- that would increase the risk of significant harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it to anyone other than the statutory agencies, where the disclosure would not be in the best interests of the child
- recorded by the player in a medical examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee or player has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited/redacted so that the person's name or identifying details are removed
- in the form of a reference given to another club.

The following actions are undertaken to ensure that Newport County AFC complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous

- A Data Protection Officer has been appointed with specific responsibility for data protection in the organisation
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:

    - Organisation name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organisational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with data protection.

11. Retention of Data

According to Data Protection principals, records containing personal information should be:

- adequate, relevant and not excessive for the purpose(s) for which they are held
- accurate and up to date
- only kept for as long as is necessary

The introduction of the General Data Protection Regulation (GDPR) in 2018 does not change the way child protection records should be stored and retained. The club will retain all records about children/adults which relate to child protection/safeguarding concerns. These records may be retained indefinitely and recent concerns across the sport sector about historic abuse or cumulative harm over periods of time from harmful behaviours evidences the need and justification for this approach in relation to safeguarding issues.

Where the club decides that the threshold has not been met for referring concerns about a child's welfare to the police or social services, NCAFC will still retain a keep a record of the issues that were raised as sometimes a picture of more serious safeguarding concerns becomes apparent over time. All files containing personal, sensitive or confidential data will be stored securely and access enabled on a strictly 'need to know' basis.

To keep personal information secure, the club maintains a central electronic recording system with restricted access. Both hard copy and electronic files will be compiled and labelled carefully.

Information about child protection concerns and referrals will be kept in a separate child protection file for each child, rather than in one 'concern log' or within a child's general records. Staff are not to use personal devices to contact children.

Record keeping and the compilation of child protection files will be started as soon as the club becomes aware of any concerns. An individual's general record will be marked where appropriate to indicate that there is a separate child protection file. A log will be maintained which records who has accessed the confidential files, when, and the titles of the files they have used.

Where there is no safeguarding or legal requirement for records to be retained for a specific period and they have not been transferred to a new club, these records will usually be kept for a period of 7 years after the individual has left the club.

The club will not keep personal data on players for any longer than is necessary. Information such as statistical data, and information that is collected to be kept as part of club records, will be kept by the club even after the child leaves. All records that are not retained will be shredded and a record made of who performed this task and when.