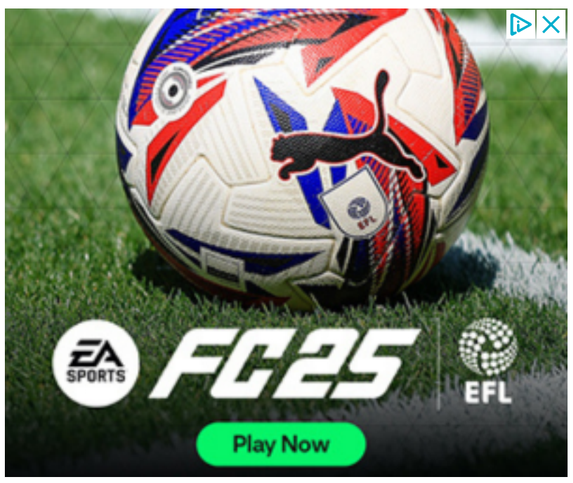

PRIVACY POLICY

CONTENTS

1. Policy Statement
2. About this Policy
3. Definition of Data Protection Terms
4. Data Protection Principles (GDPR)
5. Fair, Lawful and Transparent Processing
6. Processing for Limited Purposes
7. Notifying Data Subjects
8. Collection for Specified, Explicit and Legitimate Purposes
9. Adequate, Relevant and Non-Excessive Processing
10. Accurate Data
11. Storage Limitation
12. Data Security
13. Transferring Personal Data to a Country Outside the EEA
14. Disclosure and Sharing of Personal Information
15. Dealing with Subject Access Requests
16. Changes to this Policy

APPENDIX 1: Data Processing Activities

APPENDIX 2: Conditions for Processing Personal Data

APPENDIX 3: Conditions for Processing Special Categories of Personal Data

APPENDIX 4: Rights of Data Subjects

1. Policy Statement

1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our staff, customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1. Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

1. This policy has been drafted in line with the General Data Protection Regulations.

1. About this Policy

1. The types of personal data that Newport County AFC may be required to handle include information about employees, current, past and prospective suppliers and customers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulations ("the GDPR") (and whilst still in force and until repeal and replacement the Data Protection Act 1998 ("the Act")) and other associated regulations.

1. This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

1. This policy does not form part of any employee's contract of employment and may be amended at any time.

1. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

1. Responsibilities:
    1. The Chairman, Huw Jenkins, has ultimate responsibility for ensuring that Newport County AFC meets its legal obligations in respect of data protection. However, the Data Protection Officer, Stacey Larcombe, oversees data protection day to day.
    2. The Chief Operating Officer, Jonathan Wilsher, is responsible for:

1. Reviewing all data protection policies and procedures
2. Keeping the board and senior management updated with all data protection responsibilities, risks and issues.
3. Arranging data protection training and guidance
4. Handling any data protection questions and queries
5. Dealing with subject access requests and data breach notifications
6. Ensuring all company processing operations are sufficiently secure and compliant with all legislation
7. Ensuring accuracy and integrity of data

1. Staff are responsible for ensuring that they handle data as set out in this policy and the Data Security Policy, reading guidance notes distributed to them and ensuring they understand the requirements therein and that they make themselves fully accountable for their actions.

1. Definition of Data Protection Terms

1. **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

1. **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

1. **Personal data** means 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 factors specific to the physical, physiological, biometric, genetic, mental, economic, cultural or social identity of that natural person;

1. **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the GDPR. We are the data controller of all personal data used in our business for our own commercial purposes.

1. **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable datasecurity procedures at all times.

1. **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on Newport County AFC's behalf.

1. **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

1. **Special Categories of Personal Data** includes information about a person's racial or ethnic origin,political opinions, religious or similar beliefs, trade union membership, physical or mental health orcondition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special Categories of Personal Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

1. Data Protection Principles (GDPR)

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. 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 not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periodsinsofar as the personal data

will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

1. 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.

1. Fair, Lawful and Transparent Processing

1. The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

1. For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the GDPR. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When a special category of personal data is being processed, additional conditions must be met. When processing personal data as data controllersin the course of our business, we will ensure that those requirements are met.

1. To ensure fair and transparent processing of personal data we, as the data controller, shall provide the data subject with the following information:
   1. The period of time that the data will be stored;
   2. The right to rectification, erasure, restriction, objection;
   3. The right to data portability;
   4. The right to withdraw consent at any time;
   5. The right to lodge a complaint with a supervisory authority;
   6. The consequences of the data subject failure to provide data;
   7. The existence of automated decision-making and the anticipated consequences for the data subject.

1. Processing for Limited Purposes

1. In the course of our business, we collect and process the personal data set out in Appendix 1. This data will include data we receive directly from a data

subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

1. We will only process personal data for the specific purposes set out in Appendix 1 or for any other purposes specifically permitted by the GDPR. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

1. Notifying Data Subjects

1. If we collect personal data directly from data subjects, we will inform them about:
   1. The purpose or purposes for which we intend to process that personal data.
   2. The types of third parties, if any, with which we will share or to which we will disclose that personal data.
   3. The means, if any, with which data subjects can limit our use and disclosure of their personal data.

1. Where personal data has not been obtained directly from the data subject, we shall advise the data subject of the following:
   1. The identity and contact details of the controller and their representative;
   2. The contact details of the Data Protection Officer;
   3. The purposes, as well as the legal basis of the processing;
   4. The categories of personal data concerned;
   5. The recipients of the personal data, where applicable;
   6. The fact that the controller intends to transfer personal data to a third country and the existence of adequacy conditions.

1. We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and who the Data Protection Officer is.

1. Collection for Specified, Explicit and Legitimate Purposes

Any personal data collected will be collected for a specified, explicit and legitimate purpose 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 not be considered to be incompatible with the initial purposes.

1. Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

1. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will take every reasonable step to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

1. Storage Limitation

1. We shall keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

1. 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 subject to implementation of the appropriate technical and organisational measures.

1. Data Security

1. We will take appropriate security measures against unlawful or unauthorised processing

of personal data,and against the accidental loss of, or damage to, personal data.

1. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

1. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:
   1. **Confidentiality** means that only people who are authorised to use the data can access it.

1. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
2. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

1. Security procedures include:
   1. **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
   2. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
   3. **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
   4. **Equipment.** Data users must ensure that individual monitors do not show confidential informationto passers-by and that they log off from their PC when it is left unattended.

1. Transferring Personal Data to a Country Outside the EEA

1. Some companies we engage with to improve the services we provide will be based outside of the European Economic Area (“EEA”). Should this be the case, the transfer of personal data outside the EEA will become necessary, provided that one of the following conditions applies:
   1. The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
   2. The data subject has given their consent.
   3. The transfer is necessary for one of the reasons set out in the GDPR, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
   4. The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
   5. The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

1. In the event of clause 13.1 being activated, personal data we hold will also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff may be engaged in, amongother things, the

fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

1. Disclosure and Sharing of Personal Information

1. We share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

1. We may also disclose personal data we hold to third parties:
   1. In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.
   2. If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

1. If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

1. Dealing with Subject Access Requests

1. Data subjects must make a formal request for information we hold about them. This must be made inwriting. Employees who receive a written request should forward it to the Data Protection Officer immediately.

1. When receiving telephone enquiries, we will not disclose personal data until the identity of the data subject has been verified. Verification will involve:
   1. The data subject will be required to complete the relevant Subject Access Request form, and;
   2. Provided Identity Documents e.g. passport, driving licence etc.

1. Our employees will refer a request to the Data Protection Officer for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

1. Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

APPENDIX 1: DATA PROCESSING ACTIVITIES

Type of data	Type of data subject	Purpose of which data is held and processed	Retention period
General personal data	Employee/ Customer	Communicating with Employee and right to work checks. Communicating with customers.	6 years 10 years
Information relating to health	Employee	Recruitment, administering and managing employment where it is or may be affected by health. This includes obtaining, holding and using records of absence and sickness, medical and occupational health reports and certificates, making adjustments to your working arrangements, making decisions on your capacity for work and continuing employment, providing insurance benefits.	6 years (or in the case of a player, as long as they are registered with the Club)
Information relating to gender, race and ethnic origin	Employee / Customer / General Public	Ethnic monitoring, ensuring equal opportunity (such data is held anonymously). Information may also be apparent on photographs and CCTV which is operated for security reasons.	Used statisticsand anonymity maintained.
Information relating to criminal offences and alleged offences	Employee	Recruitment and managing employment in the light of any criminal offence or alleged offence, making decisions on continuing employment e.g. DBS checks	3 years
Other sensitive personal data	Employee / interviewee / applicant	Original purpose for obtaining data e.g. CVs	6 months unless employed by the Club
			If employed by theClub, for

Financial information	Employee	For salary payment purposes	audit purposes and until update.
CCTV imaging	Employees/ Customers/ General Public	For security and health and safety reasons.	30 days unless forlegal reasons
Credit Cardinformation	Customers	For hospitality bookings	Immediate deletion
Contact information	Customers	Marketing purposes – opt-in option Unsubscribe option	3 years

APPENDIX 2: CONDITIONS FOR PROCESSING PERSONAL DATA

Article 6 of the General Data Protection Regulations

Article 6 of the GDPR requires personal data to be processed fairly and lawfully, and, not to be processed unless one of the conditions (below) is met.

6(1)(a)	Consent of the data subject
6(1)(b)	Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
6(1)(c)	Processing is necessary for compliance with a legal obligation
6(1)(d)	Processing is necessary to protect the vital interests of a data subject or another person
6(1)(e)	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6(1)(f)	Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

In practice this means that organisations must:

1. Have legitimate grounds for collecting and using personal data
2. Not use the data in ways that have unjustified adverse effects on the individual
3. Be transparent about how it is intended to use the data by providing appropriate privacy notices when collecting personal data
4. Handle personal data only in ways they would reasonably expect
5. Make sure no unlawful activities are carried out with the data

APPENDIX 3: CONDITIONS FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

Article 9 of the General Data Protection Regulations

Article 9 of the GDPR sets out the legal bases available for processing special categories of personal data:

9(2)(a)	Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
9(2)(b)	Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
9(2)(c)	Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d)	Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
9(2)(e)	Processing relates to personal data manifestly made public by the data subject
9(2)(f)	Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
9(2)(g)	Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
9(2)(h)	Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
9(2)(i)	Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to healthor ensuring high standards of healthcare and of medicinal products or medical devices
9(2)(j)	Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

APPENDIX 4: RIGHTS OF DATA SUBJECTS

Articles 12 – 22 of the General Data Protection Regulations give rights to individuals in respect of the personal data that organisations hold about them. These include:

- The right to be informed
- The right to access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

- Rights in relation to automated decision making and profiling

The right of subject access is a wide-ranging and unless a relevant exemption applies an individual is entitled to see their personal data contained in all locations, including:

- Appraisal records
- Minutes of meetings
- Emails stored on any systems in the workplace
- References received from third parties
- Disciplinary records
- Sickness records
- Performance review notes
- Interview notes

Individuals are only entitled to see their own personal data and are not entitled to receive any information which relates to anyone else.

All requests will be monitored and fulfilled by the Data Protection Officer and processed within 48 hours.

For those who use the unsubscribe option on an email received from the Club, the request will be processed within 48 hours.

Document History Document Location

This document can be accessed from the following location:

Newport County AFC main office (hard copy)

Data Protection Officer:

Stacey Larcombe via Stacey.larcombe@Newport-county.co.uk

Created: 30.4.24 by Jonathan Wilsher (COO)

TRY A FREE
JAMESON GINGER & LIME
CLICK HERE
ENJOY RESPONSIBLY. be drinkaware.co.uk

EA SPORTS
FC25
EFL
Play Now

Carabao
£5 OFF
FREE DELIVERY AT
DRINKCARABAO.CO.UK

5 PEOPLE
HAVE AN OUT-OF-HOSPITAL
CARDIAC ARREST
EVERY 90 MINUTES
STEP UP & LEARN CPR
GET STARTED
sky bet
TAKE TIME TO THINK
GambleAware

Further Links
Company Details
Contact Us
Cookie Policy
Privacy Policy
Terms of use
Vacancies

Official iOS & Android Apps coming soon!

PURE VANS
Candour Talent. Recruitment specialists
CARDIFF CLASSIC SHIRTS
COMPCITY GIVEAWAYS
Excellence in Galvanizing WEDGE NEWPORT GALVANIZERS LTD
57 TYRES
ALFA
BEST BLINDS

#AMBER ARMY

Follow our socials

© 2025 Newport County A.F.C.

Designed & built by Other Media