AYR UNITED FOOTBALL ACADEMY

POLICY Data Protection
FOR VOLUNTEERS AND STAFF
VERSION 2.3

Created	**2018**
Reviewed by Board of Management	**August 2018**
Last review date	**August 202**
Next review date	**December 2024**

UPDATES

Date:	September 2019
Report to:	Board of Ayr United Football Academy
Report from:	Donald C Stewart
Purpose:	Annual Review
Recommendation:	No changes
Rationale:	No national changes relevant to the policy and no request from Academy personnel

Date:	August 2021
Report to:	Board of Ayr United Football Academy
Report from:	Donald C Stewart
Purpose:	Annual Review
Recommendation:	No changes
Rationale:	No national changes relevant to the policy and no request from Academy personnel

Date:	October 2023
Report to:	Board of Ayr United Football Academy
Report from:	Donald C Stewart
Purpose:	Annual Review
Recommendation:	No changes
Rationale:	No national changes relevant to the policy and no request from Academy personnel

DATA PROTECTION POLICY

This policy is intended to define the policy and principles adopted by Ayr United Football Academy ("AUFA") to govern the processing of personal data. It explains when and why we collect personal data about individuals, how we keep it secure and the data subject's rights in relation to the personal data processing. AUFA wants to ensure that employees handling personal data recognise the risks involved when dealing with personal data and fully understand the steps which need to be taken to minimise such risks and take appropriate steps to ensure that AUFA complies with the law.

AUFA are a data controller for the purposes of the GDPR and are registered with the Information Commissioner. We can be contacted by post at Ayr United Football Academy, Somerset Park, Tryfield Place, Ayr, KA8 9NB or by email at enquiries@aufa.org.uk

AUFA regards the lawful and correct treatment of personal data as crucial to the delivery of the highest quality of service and recognises that everyone has rights in relation to how their personal data is handled.

AUFA will:

- always comply with the General Data Protection Regulation ("the GDPR");
- ensure staff and other individuals are fully aware of both their rights and obligations under the GDPR; and
- implement adequate and appropriate physical and technical security measures and organisational measures to ensure the security of all information contained in or handled by AUFA including all computer systems and manual or paper systems managed by AUFA or by other parties on their behalf.

What is Personal Data?

Personal data is all recorded information about living individuals who are or could be identified from that data. In AUFA's case this includes (but is not limited to) information about:

- AUFA's employees, prospective employees and ex-employees, volunteers and interns
- Parents, carer's guardians and children who use AUFA's services
- individuals working for AUFA or volunteering with them
- individuals working for AUFA's suppliers or referral partners

These individuals are referred to as **Data Subjects**.

Personal Data covers names, identification numbers, location data, or an online identifier such as an email address, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the Data Subject. As well as written information the GDPR applies equally to images (e.g. photos, video or CCTV footage) or recorded audio information that allows individuals to be identified.

Personal Data is used by **Data Controllers** and **Data Processors**. The Data Controller is a person or entity who either alone or in common with others determines the purposes for which and manner in which personal data is processed. "Processed" simply means used.

The Data Processor is any person other than an employee of the Data Controller who processes the data on behalf of the Data Controller.

Certain categories of personal data are referred to as **Special Personal Data** (or Sensitive Personal Data. This is information concerning an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data (both in relation to physical and mental wellbeing), sex life or sexual orientation and past or spent criminal convictions. Sensitive Personal Data requires stricter protection than Personal Data and the loss or breaches of such data rightfully carries stricter punishment.

The Six Principles

There are six Principles included in the GDPR. These Principles are obligations that AUFA must follow in any processing of personal information. These apply equally to employees, volunteers and any secondees, students or interns working for AUFA. AUFA will also ensure that any suppliers (including individual consultants) comply with these Principles when working with AUFA. The GDPR says that personal data (i.e. information about living individuals held on computerised record systems or manual filing systems) must be: -

- used fairly and lawfully and processed in a transparent way;
- used for the valid purposes which we have advised you about and not used in any manner which is incompatible with those purposes (unless we have notified you and explained;
- used only to the extent necessary for the purposes we have advised you about;
- kept accurate and up to date;
- kept for no longer than necessary for the purpose which we have told you about; and
- kept secure and not be subject to unauthorised or accidental access, loss or damage or disclosure;

All AUFA staff involved in processing personal data will apply these principles.

Processing

The GDPR requires AUFA to specify the reason(s) for processing any personal data. There is a privacy statement on AUFA's website which fully and accurately reflects AUFA's processing. The Privacy Statement states the types of personal data processed; the lawful grounds for the processing; sources who it is disclosed to including any third party processors used; and the geographic reach of any processing. Changes or additional uses of personal information are discussed with AUFA's policy head to ensure that the privacy statement is kept up to date.

The GDPR states that there are six lawful grounds at least one of which must apply before personal data can be processed. These are that: -

- the individual has freely given specific and unambiguous consent to processing;
- processing is necessary for performance of a contract to which the individual is a party;
- processing is necessary to comply with a legal obligation;
- processing is necessary to protect the individual's vital interest (for example, providing emergency medical treatment in a life or death situation);
- processing is necessary for a task in the public interest or in the exercise of official authority; or
- processing is in the legitimate interests of the data controller provided their legitimate interest do not override the interests of the individual.

If none of these grounds apply any processing carried out will automatically be unlawful.

Individual's Rights

Where AUFA collects personal data directly from an individual AUFA must inform them about the purpose for which it intends to process that personal data, the types of third parties, if any, with whom that data may be shared or to which it may be disclosed. Processing will always be in line with the individual's rights under the GDPR and in particular their right to: -

- be informed about what information AUFA collects about them;
- request access to any data held about them;
- have data corrected where it is inaccurate, incomplete or not up to date;
- object to processing their data unless there are overriding legitimate grounds for us to continue doing so;

- object to decisions being taken by automated means or profiling (which largely pertains to data used for the purposes of advertising, marketing and behavioural analysis);
- have data deleted or erased where the individual believes it is no longer required for the purpose for which it was obtained, or they have validly objected to our use of that information (sometimes referred to as the right to be forgotten);
- restrict our use of their personal data, for example, where there is no longer a basis for using the information, but they don't want us to delete it; and
- request the transfer of their data to a third party (sometimes referred to as the right of portability)

Individual's may also withdraw their consent to processing personal data where the grounds of processing is based on their consent (whereupon we will stop using it for the purpose for which consent was given).

Data Subject Right of Access

Any request by an individual for access to their personal data should be made in writing to AUFA's Ayr United Football Academy, Somerset Park, Tryfield Place, Ayr, KA8 9NB. Requests from employees should be addressed in writing to the Head of Youth. AUFA will respond to requests for access to personal data within the 30 days' time limit specified in the legislation. There is no fee or charge for dealing with a Data Subject Access Request.

Disclosures

AUFA will share personal information with third parties only where this is necessary in relation to the purpose for which the information was obtained and we have notified the individual that we will do so (where there is a legitimate right to do this) or where the individual has consented to us doing so. However, AUFA will ensure that the third-party processor is compliant with the GDPR. Procedures are also in place to share personal data with appropriate authorities where required to enable them to fulfil statutory duties, e.g. when necessary to prevent or detect crime or fraud and researchers where required for research purposes, if relevant conditions are met.

Disclosure can be unlawful even if a request comes from an individual's family member, local authority, government department or the police. If an employee receives any new requests for access to personal information from third parties outside of AUFA then they should contact Head of Youth directly before any disclosure is made.

AUFA may also share anonymised statistical data with third parties. The GDPR does not apply to this type of sharing as long as individuals cannot be identified from the personal data and provided that AUFA ensures that any detailed information that could allow individuals to be identified is being withheld and that it is complying with the ICO's anonymisation code of practice.

If employees have any concerns or questions regarding the processing or use of personal data, they should contact AUFA's Head of Youth as soon as possible. If there is any doubt, employees should immediately cease to process the information.

Responsibilities

Everyone who works for AUFA (whether employed or voluntary) has a responsibility to ensure that this Data Protection Policy is fully and properly observed, to actively respond to any concerns regarding confidentiality and to ensure that personal information is processed in accordance with the rights of the individual.

The Board of Directors have overall responsibility for ensuring that AUFA works towards compliance with GDPR. Recognising that this requires the active co-operation of all staff, they will ensure that training and guidance are provided, so that all staff are able to understand and apply good information handling practices in accordance with this policy.

Much of the day to day operation of the policy is delegated to Management Team, who are responsible for making all managerial decisions in manner consistent with the spirit of the policy, for communicating the policy to all staff within their areas and supporting staff to understand their responsibilities. The Management Team must promote the development of good practice and compliance with statutory legislation and ensure that individuals managing and handling personal information are appropriately trained to do so and appropriately supervised.

Managers and supervisors have an additional responsibility to:

- set a positive example; and
- observe people and stop inappropriate practices immediately.

If a member of staff becomes aware of an actual or potential breach of security in relation to personal information, they should report it immediately to their line manager. Quick action can be crucial in mitigating the negative effects of a breach. AUFA will conduct regular audits in relation to the nature and extent of the personal data that is being stored and the uses to which such data is being put with the aim of monitoring compliance with the data protection principles described above and will exercise sanctions in respect of any breaches.

A breach of this policy by any member of staff is a disciplinary offence and may constitute gross misconduct. It is also a criminal offence for any employee, secondee, intern, consultant or supplier to access, use or disclose personal data without being authorised to do so for the purpose of their role. This may result in criminal prosecution.

Data Security & Breaches

AUFA place great importance on the security of all personal data that we hold and will always try to take appropriate precautions to protect it. We ensure that there are appropriate technical controls such as firewall and anti-virus measures are in place and carry out regular security reviews on our network. We always ensure that only authorised staff have access to personal data and that they are appropriately trained to handle it. Access will be role-based and on a need to know basis. Any third party processors will only process personal data on our instructions and are subject to a duty of confidentiality.

The GDPR requires us to put in place procedures to deal with any security breaches or suspected security breaches including reporting certain kinds of breaches to the Information Commissioner's Office within 72 hours of discovery, and in certain circumstances notifying data subjects affected of the breach. AUFA has an Incident Reporting and Security Breach Policy and procedures in place to deal with any breaches which all staff are required to comply with. A copy of this can be made available on request.

Data Retention

AUFA only retain personal data for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting or reporting requirements. To determine the appropriate retention period for personal data we refer to our Records Management Policy and Data Retention Schedule a copy of which can also be made available on request.

Overseas Transfers

Countries outside of the European Economic Area ("EEA") do not always offer the same level of protection or safeguards for processing personal data as countries within the EEA. The GDPR prohibits transfers outside of the EEA unless the transfer meets certain conditions, namely:-

- that the country to which the transfer is made has been deemed to provide an adequate level of protection by the European Commission; or
- a specific contract is in place with the overseas based service provider which has been approved by the European Commission as giving personal data the same protection it has within the EEA; or
- where the service provider is based in the United States they are party to the EU-US Privacy Shield which requires them to provide similar protection to personal data shared between EEA based service providers.

If none of the above conditions apply we may request the individual's explicit consent for the transfer but they are not obliged to give it and, if they do give it they have the right to withdraw consent at any time.

Complaints

Complaints, concerns or questions about this policy should be made to the Head of Business & Finance. However, all individuals have the right to lodge a complaint with the Information Commissioner's Office whose contact details are as follows: -

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone -0303 123 1113 or 01625 545745
Website – https://ico.org.uk/concerns

The policy will be made readily available, regularly and consistently enforced, and it will be made known to managers, supervisors, employees, volunteer workers. More detailed guidance will also be provided to staff. The Policy will be reviewed and updated regularly in response to legislative or organisational changes.

SGB Equality Impact Assessment Template

Development or review of a policy	**Name of Policy**	Data Protection Policy	
	Is this a new policy being developed or a review of an existing policy	New □	Review ■
	Others involved in the assessment	None	
	Dates(s) of EIA	August 2021	
	What is the purpose and outcomes of the policy?	To ensure that all work of the Academy operates within the context of a wider agenda seeking to eliminate unlawful discrimination against those who identify with protected characteristics, especially when dealing with data and reports and targets based upon that data.	
	Who are the customers for this policy?	All	
	How has equality been considered in the development / review of the policy so far?	This is the premium policy governing the use of data in all others. As such we are very aware that it needs to be fit for purpose and accurately observed. A group of personnel meet regularly to ensure compliance.	
	Who / what has driven this?	Annual review with irregular meetings of a data protection group which reports directly to the Board	
	Why might it be important to consider equality and the protected characteristics?	Legally it is important for us to ensure we comply with best practice on the provisions with the Equality Act and we are working with local authorities and the Scottish Football Association in contributing to their duties to those with protected characteristics under the Equality Act 2010 as well as ensuring our legal responsibilities under the same act with regards to data practices.	

Data and research	**What does the data tell you about your customers and about protected equality groups?**	At present we have not found any issue of significance
	What sources of data have you used?	All data used for our annual report and for monthly board meetings.
	What do you need to know more about?	We require to seek the views and opinions of equality groups.
	How could you find this out and who could help you?	South Ayrshire Council's Equality Forum

Consultation	**Who have you consulted with from protected equality groups?**	None
	Who else could you consult with?	South Ayrshire Council's Equality Forum
	Who can help you with this?	South Ayrshire Council

	**How does the policy contribute to the SGBs strategic equality objectives?**	Ensures compliance with both the law and the data protection duty for each of the local authorities and the governing body of the sport of football
	How could it be revised or changed to contribute more?	The opportunity to ensure it is embedded in training, reviews of its practice and specific reports to those authorities who request it.

	**How will you monitor and evaluate the policy?**	The policy shall be renewed annually

	Action	**Timescale**	**Responsibility**
	Review and suggests specific training for volunteers and staff	June 2022	EIA Lead Officer
	Reviews of its practice at annual review	June 2022	EIA Lead Officer
	Commit to respond to specific reports to those authorities who request it on the implementation of the Employment legislation associated in the Equality Act 2010	As required	EIA Lead Officer

	**Sign off**			
	Signed by Policy Lead **David White**		**Date**	
	Signed by EIA Lead Officer **Donald C Stewart**		**Date**	

Ayr United Football Academy Data Protection Impact Assessment	
Policy	Data Protection Policy
Date of assessment	August 2021
Author	Donald C Stewart
Legacy	None

DPIA process checklist

	Done?
We describe the nature, scope, context and purposes of the processing.	Yes
We ask our data processors to help us understand and document their processing activities and identify any associated risks.	Yes
We consider how best to consult individuals (or their representatives) and other relevant stakeholders.	Yes
We ask for the advice of our data protection officer.	Done
We check that the processing is necessary for and proportionate to our purposes and describe how we will ensure data protection compliance.	Yes
We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.	Yes
We identify measures we can put in place to eliminate or reduce high risks.	Yes
We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.	Yes
We implement the measures we identified and integrate them into our project plan.	Yes
We consult the ICO before processing, if we cannot mitigate high risks.	Yes
We keep our DPIAs under review and revisit them when necessary.	Yes
All of the above are covered in this, our Data Protection Policy which we make available on the website. There are specific measures in place for this guidance and it serves as guidance of our duties and responsibilities for all other policies, procedures and practice.	