January 2021

ABERDEEN SPORTS VILLAGE – DATA PROTECTION POLICY

INTRODUCTION

Aberdeen Sports Village (ASV) is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of all data held by it which affects their privacy, whether in their personal or family life, business or professional capacity and in line with the Data Protection Act (DPA).

ASV holds a range of personal data about individuals such as employees, members and others, defined as data subjects in the Act. Such data may only be processed in accordance with this policy and with the terms of ASV'S Notification to the Information Commissioner, which sets out the purposes for which ASV holds and processes personal data. Any breach of the policy may result in ASV, as the registered Data Controller, being liable in law for the consequences of the breach. This liability may extend to the individual processing the data and his/her Line Manager under certain circumstances.

ASV has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with the GDPR and the DPA. However, responsibility for compliance and the consequences of any breaches remains with the organisation.

SCOPE

1. This policy applies to all Board members, staff, students, contractors and partners working on behalf of ASV.
2. The policy applies to all personal data created, collected, stored, adapted, transferred, erased, destroyed and otherwise processed through any activity of ASV. Personal data may be held or shared in paper and electronic formats or communicated verbally in conversation or by phone.
3. The policy also applies to all locations from which ASV personal data is accessed, including home use.

DEFINITIONS

Personal data: any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. An identifier may be name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data subject: the living individual to whom the personal data relates. This includes, but is not limited to: prospective, current and former customers, current and former employees, visitors, family members where emergency and next of kin contacts are held, Board members, volunteers, event delegates, coaches and referees.

Data controller: any person, public authority, agency or other body who determines the purposes for which and the way in which any personal data is to be processed. For the purposes of this policy, ASV is the data controller and is registered with the Office of the Information Commissioner.

Processing: any operation or set of operations performed on personal data such as collection, organising, storing, adapting, retrieving, transmitting, erasing or destroying.

January 2021

Subject access request: a request for a copy of one's own personal data

Data Protection Officer: the member of staff with oversight of organisational and technical measures and controls to comply with the data protection legislation

RESPONSIBILITIES

All users of ASV information (staff, volunteers, contractors and members) are responsible for:

- completing relevant training and awareness activities provided by ASV to support compliance with the Data Protection policy and relevant procedures
- taking all necessary steps to ensure that no breaches of information security result from their actions
- reporting all suspected information security (data) breaches or incidents promptly so that appropriate action can be taken to minimise harm
- informing ASV of any changes to the information that they have provided in connection with their employment or membership, for instance, changes of address or bank account details.

The Chief Executive of Aberdeen Sports Village has ultimate accountability for ASV's compliance with data protection law and for ensuring that the Data Protection Officer is given sufficient autonomy and resources to carry out their tasks effectively.

The Director of Finance is responsible for:

- acting as the contact for the Executive Team and ensuring that staff comply with Data Protection legislation
- liaising with University of Aberdeen IT teams to ensure centrally managed IT systems and services are compliant with data protection legislation requirements.

The Data Protection Officer is responsible for:

- informing and advising senior managers and all members of ASV of their obligations under data protection law
- promoting a culture of data protection, e.g. through training and awareness activities
- reviewing and recommending policies, procedures, standards and controls to maintain and demonstrate compliance with data protection law and embed privacy by design and default across the organisation
- advising on data protection impact assessments
- monitoring and reporting on compliance to the Executive Team, the Board and committees as appropriate
- ensuring that Records of Processing and 3rd party sharing activities are maintained
- providing a point of contact for data subjects with regard to all issues related to their rights under data protection law
- investigating personal data breaches, recommending actions to reduce their impact and likelihood of recurrence
- acting as the contact point for and cooperating with the Information Commissioner's Office on issues relating to processing;

Where permissible under the legislation, some of these duties may also be undertaken by the Director of Finance, or other arrangements may be made for oversight of these duties.

All team managers are responsible for implementing this policy within their business areas and for adherence by staff. This includes:

- managing access rights for information assets and systems to ensure that staff, contractors and agents have access only to such personal data is necessary for them to fulfil their duties
- ensuring that all staff in their areas of responsibility undertake relevant and appropriate training and are aware of their responsibilities for data protection
- ensuring that staff responsible for any locally managed IT services liaise with the University of Aberdeen's IT staff to put in place equivalent IT security controls
- assisting the Data Protection Officer in maintaining accurate and up to date records of data processing activities
- ensuring that they and their staff cooperate and support the Data Protection Officer in relation to subject access requests and other requests relating to personal data where the data is managed by their business area; and
- recording data protection and information security risks on the organisation's Risk Register and escalating these as necessary.

The Executive Team will ensure that staff roles and responsibilities are clearly defined in terms of data protection and that Job Descriptions reflect this.

POLICY STATEMENT

ASV is committed to applying the principles of data protection to the management of personal data at all stages of its lifecycle. The following policy objectives will be adopted:

We will process data fairly and lawfully This means we will

- only collect personal information where it is necessary so that we can deliver our functions and services
- ensure that if we collect personal data for a specific purpose, or purposes, we will not reuse it for a different purpose that the individual did not agree to or expect
- rely on consent as a condition for processing only where we obtain specific, informed and freely given consent that is affirmative and documented.

We will tell data subjects what is done with their personal data. As we collect personal data we will explain, in simple terms:

- What we collect and what we use it for
- the lawful basis we rely on to process the data (for each purpose)
- Whether we use it for any other legitimate purpose
- Whether the data is needed to meet a statutory or contractual requirement
- The source of the data, including where we receive it from third parties
- Whether we use automated decision making or profiling
- How we will protect the data
- Who we may disclose it to
- How long we keep the data for and how we dispose of it when no longer required
- How data subjects can update the personal data we hold
- How data subjects can exercise their rights
- Who our Data Protection Officer is and how they can be contacted

DATA SECURITY

All users of personal data within ASV must ensure that personal data are always held securely and are not disclosed to any unauthorised third party either accidentally, negligently or intentionally.

PRIVACY NOTICES

ASV will use privacy notices to let data subjects know what is done with their personal data. Privacy notices are published on the ASV website and are available to staff and customers from their first point of contact with ASV. Any processing of staff or customer data beyond the scope of the standard privacy notices will mean that a separate privacy notice is required. We will regularly review these privacy notices and will inform the relevant data subjects of any changes that may affect them.

DATA RETENTION

Personal data will not be kept longer than necessary, for the purposes for which it was originally collected. This applies to all personal data, whether held on core systems, local PCs, laptops or mobile devices or held on paper. If the data is no longer required, it will be securely destroyed or deleted, in line with the ASV retention schedule.

DATA PROTECTION BY DESIGN AND DEFAULT

Under the GDPR and the DPA, ASV has an obligation to consider the impact on data privacy during all processing activities. ASV will implement appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy.

DATA PROTECTION IMPACT ASSESSMENT

When considering new processing activities or setting up new procedures or systems that involve personal data, ASV will consider potential privacy issues at the earliest stage and a Data Protection Impact Assessment (DPIA) will be conducted. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection control requirements are not an after-thought.

ANONYMISATION AND PSEUDONYMISATION

Further mechanisms of reducing risks associated with handling personal data are to apply anonymization or pseudonymisation. Wherever possible, ASV will anonymise, or where that is not possible pseudonymise, personal data.

DATA SUBJECT RIGHTS AND SUBJECT ACCESS REQUESTS

ASV will uphold a data subject's rights to:

- obtain a copy of the information comprising their personal data (known as making a subject access request)
- have inaccurate personal data rectified and incomplete personal data completed
- have their personal data erased when it is no longer needed, if the data has been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data
- restrict the processing of their personal data until a dispute about the data's accuracy or use has been resolved, or when ASV no longer needs to keep personal data but the data subject needs the data for a legal claim

- data portability (if applicable): where a data subject has provided personal data to ASV by consent or contract for automated processing and asks for a machine-readable copy or to have the data sent to another data controller
- object to and prevent further processing of their data for the legitimate interests or public interest unless ASV can demonstrate compelling lawful grounds for continuing
- prevent processing of their data for direct marketing
- object to decisions that affect them being taken solely by automated means (if applicable); and
- claim compensation for damages caused by a breach of data protection law.

Subject access requests (requests for a copy of one's own personal data) will be responded to by ASV, free of charge, within one month of the request being received. ASV may charge a reasonable administrative fee to cover costs if the request is manifestly unfounded or excessive, or if an individual requests further copies of their data. A further two months to respond may be granted in exceptional circumstances, for example if the request is complex or a number of requests are received from the same person.

ASV will also ensure it communicates to all data subjects their right to lodge a complaint with the Information Commissioner's Office.

DATA SHARING

When personal data is transferred internally, ASV recipients will only process the data in a manner consistent with the original purpose for which the data was collected. If personal data is shared internally for a new and different purpose, a new privacy notice will be provided to the relevant data subjects.

When personal data is transferred externally, a legal basis must be determined and a data sharing agreement between ASV and the third party must be signed, unless disclosure is required by law, such as certain requests from the Department for Work and Pensions or Inland Revenue, or the third party requires the data for law enforcement purposes.

DIRECT MARKETING

Direct marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For ASV, this will include notifications about events, fundraising, selling goods or services. Marketing covers all forms of communications, such as contact by post, fax, telephone and electronic messages, whereby the use of electronic means such as emails and text messaging is governed by the Privacy and Electronic Communications Regulations 2003. ASV will ensure it complies with relevant legislation every time it undertakes direct marketing and will cease all direct marketing activities if an individual requests it to stop.

DATA PROTECTION TRAINING

ASV will ensure all staff take part in mandatory data protection training to enable them to comply with data privacy laws.

DATA PROTECTION BREACHES

ASV is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against

accidental loss, destruction or damage of the data. ASV will make every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

The ASV Data Protection Officer and Director of Finance must be informed of any data breach incident immediately on discovery. The DPO and senior managers will investigate and decide if the incident constitutes a data protection breach. If a reportable data protection breach occurs, ASV is required to notify the Information Commissioner's Office as soon as possible, and not later than 72 hours after becoming aware of it.

RELATIONSHIP WITH OTHER POLICIES

This policy has been formulated within the context of the following ASV and UoA documents:

- Information Security Policy
- Acceptable Use Policy

Related ASV and UoA policies must be read in conjunction with this Data Protection Policy.