DATA PROTECTION POLICY

IAPS is registered under the Data Protection Act and GDPR.

About this policy

Everyone has rights with regard to the way in which their personal data is handled. During the course of the association's activities, it collects, stores and processes personal data about staff, members, course and sports events participants, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Any breach of this policy may result in disciplinary action.

This policy sets out the basis on which the association will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time.

General statement of the association's duties

The association is required to process relevant personal data regarding workers as part of its operation and shall take all reasonable steps to do so in accordance with this policy.

Data Protection Controller

The association has appointed the Finance and Operations Director as the Data Protection Controller (DPC) who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the GDPR Act 2018. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Controller.

The principles

Anyone processing personal data must comply with the eight enforceable principles of good practice as enshrined within the GDPR Act 2018. These provide that personal data must be:

- Lawfulness, fairness and transparency

  Transparency: Tell the subject what data processing will be done. Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)].

- Purpose limitations

  Personal data can only be obtained for "specified, explicit and legitimate purposes"[article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

- Data minimisation

  Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. In other words, no more than the minimum amount of data should be kept for specific processing.

- Accuracy

Data must be “accurate and where necessary kept up to date” [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

- Storage limitations

The regulator expects personal data is “kept in a form which permits identification of data subjects for no longer than necessary” [article 5, clause 1(e)]. In summary, data no longer required should be removed.

- Integrity and confidentiality

Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage” [article 5, clause 1(f)].

Personal data

Personal data covers information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, pupils and their parents, suppliers and marketing and business contacts. It includes expressions of opinion about the individual, any indication of someone else’s intentions towards the individual, information necessary for employment such as the worker’s name and address and details for payment of salary.

Processing of personal data

The association’s policy is to process personal data in accordance with the applicable data protection laws as set out above. All staff have a personal responsibility for the practical application of this policy.

Staff should generally not process personal data unless:

- The individual whose details are being processed has consented to this;
- The processing is necessary to perform the association’s legal obligations or exercise legal rights, or
- The processing is otherwise in the association’s legitimate interests and does not unduly prejudice the individual’s privacy.

When gathering personal data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. There are limited exceptions to this notice requirement. In any case of uncertainty as to whether a notification should be given, staff should contact the DPC.

Sensitive personal data

The association may, from time to time, be required to process sensitive personal data regarding a worker. Where sensitive personal data is processed by the association, the explicit consent of the worker will generally be required in writing.

The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the DPC for more information on obtaining consent to process sensitive personal data.

Processing of credit card data

The association complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Finance and Operations Director

Accuracy, adequacy, relevance and proportionality

Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask the association to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the DPC.

Staff must ensure that personal data held by the association relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the DPC so the association's records can be updated.

Rights of individuals

Individuals have the right of access to information held by the association, subject to the provisions of the GDPR Act 1998. Any individual wishing to access their personal data should put their request in writing to the DPC. Employees who receive a written request for personal data should forward it to the DPC immediately.

The association will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 30 days. The information will be imparted to the individual as soon as is reasonably possible after it has come to the association's attention. It should be noted that there are certain restrictions on the information to which individuals are entitled under applicable law.

Staff should not send direct marketing material to someone electronically (eg. by email) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their personal data for direct marketing purposes and should notify the DPC about any such request. Staff should contact the DPC for advice on direct marketing before starting any new direct marketing activity.

Exemptions

Certain data is exempted from the provisions of the GDPR Act which includes the following:-

- Safeguarding
- The prevention or detection of crime
- The assessment of any tax or duty

- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the association

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPC.

Accuracy

The association will endeavour to ensure that all personal data held in relation to individuals is accurate and kept up to date. Individuals must notify the DPC of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased.

Timely processing

The association will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required.

Enforcement

If a member of staff believes that the association has not complied with this policy or acted otherwise than in accordance with the Data Protection Act, the member of staff should utilise the association grievance procedure and should also notify the DPC.

Data security

The association must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to both staff, members and persons participating in events. As such, no member of staff is permitted to remove personal data from association premises, whether in paper or electronic form and wherever stored, without prior consent of the Chief Executive or the Finance and Operations Director. Where a worker is permitted to take data offsite it will need to be encrypted.