DATA PROTECTION POLICY

CONTENTS

1. BACKGROUND

1.1 The Policy is informed by the General Data Protection Regulation (GDPR) which came into force on the 25th May 2018 and all other applicable laws and regulations relating to processing of personal data and privacy (described collectively as data protection laws).

1.2 Data protection laws all require that the personal data is processed in accordance with specific data protection principles. New data protection law provides stronger rights for individuals to be informed about how organisations use their personal data and greater control over how their personal data is used.

1.3 Data protection laws in the UK are regulated by the Information Commissioner's Office (ICO). The ICO has extensive powers, including the ability to impose civil fines of up to Euros 20 million or 4% of group worldwide turnover, whichever is higher.

1.4 The Policy identifies our responsibilities under the data protection laws and the steps we will take not just to meet legal requirements but to build a culture of privacy and transparency where individual rights and freedoms are always at the forefront of everything we do with personal information.

2. PURPOSE

2.1 This policy interprets how our employees, coaches and volunteers, who are acting on behalf of Falcon, must comply with data protections laws in the context of work or voluntary activities for Falcon.

2.2 The key aims of the policy are to: -

2.2.1 Identify our legal responsibilities under data protection laws and how we will comply;

2.2.2 Set out specific roles and individual responsibilities;

2.2.3 Ensure all employees, coaches and volunteers understand the importance of maintaining privacy and respecting individual rights and freedoms in relation to their personal data; and

2.2.4 Provide clarity and establish uniformity in data protection practice.

3. SCOPE

3.1 This policy covers all personal information we hold about employees, volunteers, gymnasts, parents and anyone else whose data we process.

3.2 This policy applies to both personal data and sensitive personal data that is held in an automated (electronic) format. This includes:

3.2.1 All electronic devices, including desk top computer, laptops and tablets

3.2.2 Text messages and any other personal information held on company devices

3.2.3 Imagery (photographs and video footage)

3.3 The policy also applies to manual filing systems where personal data are accessible according to specific criteria e.g. name, ID etc.

4. POLICY STATEMENTS

4.1 Falcon is committed to complying with data protection laws and respecting the privacy rights and freedoms of individuals. We believe that ensuring personal information is processed lawfully, fairly and transparently, is of matter of strategic importance and a key departmental responsibility.

4.2 It is vital for the growth and sustainability of our organisation to maintain the trust and confidence of our employees, coaches, volunteers, gymnasts, parents and others whose data we process.

4.3 We recognise our responsibilities under data protection laws and will comply with the following data protection principles and ensure that any personal data is:

4.3.1 Processed lawfully, fairly and in a transparent manner, and only if certain specified conditions are met;

4.3.2 Collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes (purpose limitation);

4.3.3 Adequate and relevant, and limited to what is necessary to the purposes for which it is processed (data minimisation);

4.3.4 Accurate and where necessary kept up to date;

4.3.5 Kept for no longer than is necessary for the purpose (storage limitation); and

4.3.6 Processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures (integrity and security).

4.4 In addition, we recognise that we are required to demonstrate how we are accountable for complying with these principles and will:

4.4.1 Maintain a register of all personal data assets we hold;

4.4.2 Minimise the access to personal data to only those individuals who need the information to undertake their roles.

4.4.3 Only process personal data where we have a lawful basis to do so and it is necessary for the specific purpose.

4.4.4 Before relying on legitimate interests as a lawful basis, assess whether the processing can be achieved in a balanced way that safeguards individual interests, rights and freedoms.

4.4.5 Only process sensitive personal information where there is a lawful basis for doing so and an additional condition for processing sensitive information applies.

4.4.6 Only process criminal offences and convictions information where we have a legal obligation to do so.

4.4.7 Provide transparent information to all data subjects, including those who are children or otherwise vulnerable about the processing we undertake and their individual rights in a concise, intelligible and easily accessible form, using clear and plain language.

4.4.8 Ensure we have effective systems and processes to enable data subjects to easily assert their individual rights.

4.4.9 Implement appropriate technical and organisational measures to keep personal information secure, minimising the likelihood of unauthorised or unlawful processing and protecting against accidental loss, destruction or damage.

4.4.10 Ensure that where we undertake a processing operation on behalf of another controller we implement appropriate technical and organisational measures to maintain the security and integrity of their data and process it in accordance with applicable data protection laws.

4.4.11 Maintain additional documentation as required to demonstrate our accountability under data protection laws.

4.4.12 Document and continually monitor the security measures in place for all personal data we hold and ensure they continue to provide an appropriate level of security paying due regard to the specific risks associated with the processing.

4.4.13 Take timely action to contain any personal data breaches and notify the Information Commissioner and affected data subjects where required to do so under data protection laws.

4.4.14 Ensure all employees, coaches and volunteers are provided with training that is appropriate to their role and responsibilities as set out in this policy; and

4.4.15 Take appropriate action against any individual who fails to comply with the policy, procedures and operational guidance.

5. DEFINITIONS

The following are key definitions and terms used in this policy:

5.1 **Personal data/information** means any information relating to an identifiable person who can be directly or indirectly identified (i.e. with reference to other information available or obtainable) by reference to an identifier

5.2 **Identifiers** are personal information such as a name or ID number but can also include location data or online identifier or one or more factors such as physical, physiological, genetic, economic or social identity of that individual.

5.3 **Processing** means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with personal data.

5.4 **Data subject** means the living individual to whom the relevant personal data relates.

5.5 **Data controller** means the legal person i.e. the company or individual who decides how personal data is used. For example, we will always be a data controller in respect of personal data relating to our employees.

5.6 **Data processor** is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, For example, an outsourced payroll provider will be a data processor.

5.7 **Lawful basis/bases** is/are the legal reason(s) that permits the processing of personal data. Special categories of personal data are exempt from processing unless a further condition applies. Criminal records information can only be processed where the data is processed in an official capacity, or where there is a specific national legal that authorisation.

5.8 **'Legitimate interests'** is one of the six legal bases which can be relied upon where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.9 **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes given by statement or by a clear affirmative action, that signifies agreement to the processing of their personal data.

5.10 **Sensitive personal data** is referred to in the GDPR as special categories of personal data and means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation. Special categories of personal data do not include information about criminal offences and convictions, but the GDPR requires similar safeguards for the processing of this type of data.

5.11 **Criminal records information** means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

5.12 **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

6. ROLES & RESPONSIBILITIES

6.1 The Board is ultimately responsible for ensuring we conduct our data processing activities in line with data protection laws. The Head of Falcon is responsible for supporting the implementation of the policy and ensuring it is effectively resourced.

6.2 Head of Falcon

The Head of Falcon is directly accountable for managing the privacy risks within Falcon but may delegate specific responsibilities to an appropriately trained and competent employees, coaches or volunteers within Falcon. Responsibilities include:

6.2.1 Ensuring that all employees, coaches and volunteers who undertake processing activities understand their responsibilities under the Policy and complete the required training.

6.2.2 Responding to audit recommendations.

6.2.3 Ensuring the required documentation is completed before undertaking any new processing activities.

6.2.4 Ensuring appropriate action is taken to address any repeated non-compliance with the Policy and operational guidance.

6.3 Data Owners

All personal data assets have a data owner who is responsible for maintaining the asset in accordance with the data protection principles. Data Owners must ensure the asset is

6.3.1 Accurate and kept up to date.

6.3.2 Only accessible by those who need access to undertake their role.

6.3.3 Stored in the appropriate location.

6.3.4 Reviewed and deleted or archived in accordance with the applicable retention period.

6.4 All Employees, Coaches and Volunteers

Everyone is personally responsible for ensuring they conduct their own work activities in accordance with this policy and must:

6.4.1 Read and confirm understanding of the Policy.

6.4.2 Only carry out processing activities that are documented unless the Head of Falcon has given prior authorisation.

6.4.3 Only access personal information that is required for the role.

6.4.4 Ensure personal information and actions relating to this data are recorded accurately in both manual and electronic records.

6.4.5 Report any actual or suspected personal data breaches or significant near misses to the Head of Falcon without delay.

6.5 Monitoring

This Policy will be regularly monitored to ensure it remains up to date. The following situations are also likely to evoke a review of the policy:

6.5.1 Any changes in the law or relevant guidance.

6.5.2 Following a significant civil or criminal case or enforcement action involving another organisation; and

6.5.3 A direct intervention by the ICO.

6.6 Reporting & Communications

6.6.1 The policy needs to be specifically communicated to the following individuals and groups:

6.6.1.1 All Falcon employees, coaches and Board members.

6.6.1.2 All Falcon volunteers who require access to personal information as part of their role.

6.6.2 The Head of Falcon is responsible for communicating the policy.

6.6.3 All individuals must sign to confirm that they have read the policy and understand how it relates to their individual responsibilities.

7. PROCEDURES

The Head of Falcon has overall responsibility for ensuring the following procedures are applied in respect of personal data we process.

7.1 Lawful processing of personal data

7.1.1 Before commencing any processing activities for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis (or bases).

7.1.2 Except where the processing is based on consent, we will satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

7.1.3 We will regularly review the processing activities we undertake to ensure that the identified legal base or bases continue to be appropriate.

7.2 Legitimate interests

7.2.1 We recognise our additional responsibility for considering and protecting people's rights and interests where we are considering legitimate interests as the legal basis for a specific activity.

7.3 Sensitive Personal Information

7.3.1 We will only process sensitive personal information if we have a lawful basis for doing so.

7.3.2 We will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

7.4 Documentation and records

7.4.1 We will document any processing activities that involve sharing or disclosing personal information with a third-party.

7.5 Right to be informed

7.5.1 Individuals have the right to be informed about the collection and use of their personal data. We will provide this information in a concise, transparent, intelligible, easily accessible format using clear and plain language.

7.5.2 Where this information is provided by or relates to a child or someone who is known to be vulnerable for another reason, we will take steps to ensure this information is provided in a format that is appropriate to their age and ability to understand.

7.5.3 Our privacy policy provides the following information:

- Our name and contact details of our organisation
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.

7.5.4 Falcon's privacy policy is published on the Falcon website at

https://www.falcongym.com/policies/privacy-policy/

7.6 Other individual rights

7.6.1 Under data protection laws, data subject have the following additional rights in relation to their own personal data:

7.6.1.1 the right of access to personal data and other supplementary information (this is known as a data subject access request, DSAR or SAR)

7.6.1.2 the right to rectification

7.6.1.3 the right to erasure (also known as the right to be forgotten)

7.6.1.4 the right to restrict processing
7.6.1.5 the right to data portability
7.6.1.6 the right to object
7.6.1.7 rights in relation to automated decision making and profiling (It is not expected that this right will impact upon as we do not process personal data by automated means).

7.6.2 Data subjects can exercise their rights in writing or verbally. There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the ICO and/or legal action by the affected individual.

7.6.3 When a request is received, a response should be provided without undue delay and in any event within one month of receipt of the request. The time limit starts from the day after the request is received (irrespective of whether the day after is a working day or not) until the corresponding calendar date in the next month (or before if the next month has fewer days).

7.7 Requests for information by someone with parental responsibility for the data subject

7.7.1 Although individual rights under data protection laws rest with the data subject, as many of our beneficiaries are children, it is more likely that requests will come from someone who has parental responsibility. Where the request is simple or routine, the employee, coach or volunteer should verify that the person requesting the information holds parental responsibility for the data subject. Where information is being requested by an adult that we are unable to verify holds parental responsibility for the child, this information should not be provided without the specific authority of the data subject. If the data subject is under 13, this authority can be provided by the adult who is named on the account.

7.7.2 If the information being requested is sensitive or the employee, coach or volunteer has any concerns relating to the provision of personal information, no information should be provided, and the matter must be referred to the Head of Falcon for guidance. Where the data subject is over 13 and there is uncertainty about their wishes regarding the disclosure of sensitive information to a parent, the data subject's authority must be obtained prior in any information being shared.

7.8 Other third-party requests

7.8.1 Data protection laws do not prevent a third party making a subject access request on behalf of a data subject. Any request that is made by a third party other than someone with parental responsibility for the data subject should always be brought to the attention of the Head of Falcon.

7.8.2 It is the responsibility of the third party to demonstrate that they have the data subject's authority to act on their behalf. In responding, we will need to be satisfied that the third party making the request has this authority and can request written authority from the data subject or a more general power of attorney where appropriate.

7.8.3 Where the Head of Falcon believes that the data subject has not understood fully what information will be disclosed to the third party who has made the request, the response will be sent directly to the data subject. The individual in question can then choose to share the information with the third party after having had a chance to review it first. Where a request is made by third party (e.g. a legal advisor), we will take steps to verify that the request was, in fact, instigated by the data subject and that the third party has the proper authority to act on their behalf.

7.9 Notification of a request

7.9.1 Any written or verbal request that is not simple of routine must be brought to the attention of the Head of Falcon without delay.

7.9.2 If an employee, coach or volunteer receives a verbal request, even if they are uncertain as to the nature of the request, they should make a written record of all relevant details and explain that they will refer the matter to the Head of Falcon who will contact them.

7.9.3 If possible, the individual making the request should be encouraged, if they are willing, to confirm the request in writing to the Head of Falcon. If the individual is requesting a copy of information that we may hold about them, they should, if they are willing, complete a request in writing. If the individual wishes to object to a processing activity carried out in our legitimate interests, they should be encouraged to complete an objection in writing.

7.10 Next steps

7.10.1 Where we refuse to respond to a request, we must explain why to the individual, informing them of their right to complain to the ICO without undue delay and at the latest within one month.

7.11 Searches

7.11.1 Where the requested information may be located in several filing and/or network systems and on mobile devices it is important to identify at the outset the type of information requested to enable a focused search.

7.11.2 Although the data subject is under no obligation to assist, if we do not receive a useful clarification or any response at all, we will need to search all information we hold to comply with the request including:

7.11.2.1 All electronic systems (e.g. databases, networked and non-networked computers, servers, emails, CCTV and photography and video footage);

7.11.2.2 All company mobile phones and tablets

7.11.2.3 Manual/paper filing systems (but only if they are 'structured filing systems' - see below); and

7.11.2.4 Any electronic data of data held in structured filing systems by our data processors.

7.11.3 All relevant systems will be searched using the individual's name, address, telephone number, email address or other information specific to that individual. In each case the scope of the search may be different.

7.11.4 Information that is not part of a structured filing system, does not amount to personal data and will fall outside the scope of personal data under the data protection laws, and therefore will not be caught by the rights of data subjects.

7.12 Right of Access

7.12.1 Data protection laws provides individuals the right to obtain:

7.12.1.1 confirmation that their personal data is being processed.

7.12.1.2 access to their personal data; and

7.12.1.3 access to other supplementary information.

7.12.2 The individual is entitled to receive a description of the following:

7.12.2.1 the purposes for which we process the data.

7.12.2.2 the categories of personal data we process about them.

7.12.2.3 the recipients to whom we may disclose the data.

7.12.2.4 the duration for which the personal data may be stored.

7.12.2.5 the rights of the data subject under the data protection laws.

7.12.2.6 any information available regarding the source of the data if it was not collected from the data subject direct.

7.12.2.7 the right of the data subject to make a complaint to the supervisory authority for data protection.

7.12.2.8 the logic behind any automated decision we have taken about him or her (see below), the significance and consequences of this automated processing.

7.12.3 We must provide the information constituting the individual's personal data which is within the scope of their request. We must provide this information in an intelligible form and technical terms, abbreviations and codes must be explained, and where the request was made electronically, we can, unless the data subject specifies otherwise, also provide the information in electronic form.

7.13 Redactions

7.13.1 Where we are providing information to an individual where they have made a subject access request, they are only entitled to their personal data. Although we may provide non-personal information on a discretionary basis, they are not entitled to see information which relates to other individuals and such information will usually be redacted unless it is already known by the data subject.

7.13.2 Sometimes information that is determined to be personal data about the person making the request might also include information that identifies or is the personal data of another person e.g. a letter of complaint. In some cases, it is not possible to redact the information about the other person but the information can be disclosed if the other person has consented.

7.13.3 Where the other person has not consented, the Head of Falcon will consider whether it would be reasonable in the circumstances to disclose this information to the person making the request.

7.13.4 In making this decision, we will consider:

- 7.13.4.1 Whether asking for consent might reveal the identity of the individual making the request and if we owe that person a duty of confidentiality.
- 7.13.4.2 What steps we have taken to obtain the consent of the other person.
- 7.13.4.3 Any specific reason why the other person has refused their consent.
- 7.13.4.4 Any reason why the other person's consent cannot be obtained e.g. because they are incapable of giving it due to illness or incapacity.
- 7.13.4.5 If the other person is the source of the information.
- 7.13.4.6 If there is an imbalance of power or authority between the person making the request and the other person and if the data may be used in a way that is to the other person's disadvantage.
- 7.13.4.8 Whether the information is generally known by the individual making the request; and where the person making the request has a legitimate interest in the disclosure of the other person's information which they have made known to us.

7.13.5 If we decide that the other person's information should be withheld, we still have to provide as much information as we can without compromising the other person's identity. Therefore, redactions should be limited to those specifically required to protect the other person's identity.

7.14 Exemptions to the right of subject access

7.14.1 There are certain circumstances where an exemption to providing personal data in response to a subject access request may apply.

7.14.2 All following exemptions will be considered and applied on a case-by-case basis after a careful consideration of all the facts.

- 7.14.2.1 Crime detection and prevention
- 7.14.2.2 Confidential references
- 7.14.2.3 Legal professional privilege
- 7.14.2.4 Management forecasting
- 7.14.2.5 Company negotiations

7.15 Right to Erasure

7.15.1 Data subjects have the right to request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

7.15.2 The right to erasure is not an absolute right and applies only as follows:

7.15.2.1 where personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

7.15.2.2 when the data subject withdraws consent (but only to the extent that consent is the only basis for processing their personal data);

7.15.2.3 where the data subject objects to the processing of their personal data and there is no overriding legitimate interest for continuing the processing.

7.15.2.4 where the personal data was unlawfully processed.

7.15.2.6 where the personal data has to be erased in order to comply with a legal obligation; and where the personal data is processed in relation to the offer of information society services to a child.

7.15.3 There are some specific circumstances where the right to erasure does not apply, and we can refuse to deal with a request if we require the personal information:

7.15.3.1 to exercise the right of freedom of expression and information.

7.15.3.2 to comply with a legal obligation or for the performance of a public interest task or exercise of official authority.

7.15.3.3 for public health purposes in the public interest.

7.15.3.5 archiving purposes in the public interest, scientific research historical research or statistical purposes; or the exercise or defence of legal claims.

7.16 Right to rectification

7.16.1 An individual has the right to ask us to:

7.16.1.1 correct inaccurate personal data.

7.16.1.2 complete information if it is incomplete; and

7.16.1.3 delete personal data which is irrelevant or no longer required for our purposes.

7.16.2 Where information has been provided to a third-party, we must inform them of the rectification request where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

7.17 Right to Restrict Processing

7.17.1 An individual is entitled to require us to stop or not begin processing their personal data. When processing is restricted, we are permitted to store their personal data, but not further process it except in the exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. We can retain just enough information about the individual to ensure that the restriction is respected in future.

7.17.2 We are required to restrict the processing of personal data in the following circumstances:

7.17.2.1 Where a data subject challenges the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data;

7.17.2.2 Where a data subject has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our legitimate grounds override those of the individual.

7.17.2.4 When processing is unlawful and the individual opposes erasure and requests restriction instead; and if we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

7.17.3 This right to restrict processing does not apply if the individual has entered into a contract with us and the processing is necessary for the fulfilment of that contract.

7.17.4 Where a request to restrict processing is received, the Head of Falcon will inform the data subject of the action taken and specifically advise when we decide to lift a restriction on processing e.g. if an individual contested our right to process their personal data on legitimate interest grounds and we subsequently found that there was compelling justification to continue to process the individual's data.

7.17.5 If we have disclosed the restricted personal data to third parties, the Head of Falcon will inform them if we have agreed to erasure any personal data, unless it is impossible or involves disproportionate effort to do so.

7.18 The Right to Data Portability

7.18.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

7.18.2 The right to data portability only applies:

7.18.2.1 to personal data an individual has provided to a data controller.

7.18.2.3 where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means.

7.18.3 We must provide the personal data in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data. The information must be provided free of charge.

7.18.4 If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

7.19 Right to Object

7.19.1 Individuals have the right to object to processing based on legitimate interests.

7.20 Deleting personal data in the normal course

7.20.1 We are only required to supply information in response to an exercise of individual rights that was processed at the date of that request. However, we are allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of request in relation to a Right.

7.20.2 In no other circumstance will we amend or delete data because we do not want to supply it or because of the exercise of a right.

7.21 Information security

7.21.1 We recognise our responsibility to implement appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

7.22 Storage and retention of personal information

7.22.1 Personal information (and sensitive personal information) will be kept securely.

7.22.2 We will maintain a retention schedule that sets out the specific periods for which we will retain each type of personal data. The retention periods will take account of any statutory requirements as well as other lawful reason why we need to retain the information and to securely dispose of any personal information where we no longer have a lawful reason to hold it.

7.22.3 Personal information (and sensitive personal information) will not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.

7.22.4 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

7.22.5 All information will be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

7.22.5 Hard copy and electronically-held documents and information will be disposed of by shredding or deleted at the end of the retention period.

7.23 Data Breaches

7.23.1 We will report to the Information Commissioner's Office without undue delay and within 72 hours of becoming aware of it any breach that results in a risk to the rights and freedoms of individuals. We will also notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms.

7.24 Training

7.24.1 We will ensure that all employees, coaches and volunteers receive appropriate training regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

7.25 Consequences of failing to comply

7.25.1 Failure to adhere to this policy could result in individuals being criminally liable for deliberate unlawful disclosure of personal information. This may result in criminal prosecution and/or disciplinary action. We take compliance with this policy very seriously. Failure to comply with the policy:

7.25.1.1 puts at risk the individuals whose personal information is being processed; and

7.25.1.3 carries the risk of significant civil and criminal sanctions for the individual and the Company; and may, in some circumstances, amount to a criminal offence by the individual.

7.25.2 We will ensure that all employees, coaches and volunteers comply with this policy, operational guidance and procedures as far as they are relevant to their individual role and responsibilities and will use the provisions contained in terms and conditions of employment and specific data processing clauses to carry out any investigation and where appropriate take disciplinary action where there is a concern that any individual may have acted in a way that does not comply our policy and/or data protection law. Where it is determined, in accordance with the relevant disciplinary procedures that an individual has failed to comply, this could lead dismissal or termination of a contract or voluntary position.

Reviewed April 2026