1 Harbourmead, Harbour Road
Portishead Bristol BS20 7AY
Tel: 01275 840077
Website: www.thegymacademy.co.uk
Email: admin@thegymacademy.co.uk

THE ACADEMY OF GYMNASTICS

Inspiring Children

Data Protection Policy

Contents

1. Introduction 3
2. Purpose 3
3. Application 3
4. What is personal information? 3
5. The three key elements of Data Protection Legislation 3
5.1 Data Protection Principles 4
5.2 Rights of Individuals 5
5.3 Lawful Basis for Processing 5
6 What personal information we collect and how we use it 5
6.1 What we need 5
6.2 Why we need it 6
7. Special Category Information 6
8. Handling personal information, lawfully, fairly and transparently 6
9. Consent 7
10. Contract 7
10.1 When is processing 'necessary' for a contract? 7
11. Legal Obligation 8

12. Vital Interests 8
12.1 What are 'vital interests'? 8
12.2 When is vital interests likely to apply? 8
13. Public Task 8
14. Legitimate Interests 8
15. Fair treatment 9
16. Minimum amount of personal data 9
17. Accurate and kept up to date 10
18. Marketing 10
19. Children 10
20. Subject Access Requests 11
21. Requests for information from law enforcement agencies 11
22. Data security 11
23. Managing and monitoring staff 12
24. PCI-DSS 12
25. Outsourcing 12
26. Restrictions on transferring information to countries outside the UK and EEA 13
27. Data Incidents 13
27.1 Data loss 14
28. Data retention 14
29. Secure disposal of records and computer equipment 14
30. Individual responsibilities 15
31. Training 15
32. Data Protection Impact Assessments (DPIA) 15
32.1 What is a data protection impact assessment? 15
32.2 When do we need to conduct a DPIA? 16
32.3 What does a DPIA cover? 16
33. Data Protection Officer 16
34. Monitoring & Reporting 16
35. Review 16

1. Introduction

Data Protection Legislation governs the processing (i.e. obtaining, holding, organising, recording, retrieval, use, disclosure, transmission, combination and destruction) of personal and sensitive data (i.e. information relating to a living individual - the data subject) and sets out the rights of individuals whose information is processed in manual or electronic form or held in a structured filing system.

The General Data Protection Regulation (GDPR) is European wide data protection legislation that requires organisations working with individuals based in the European Economic Area or whose business is based in the European Economic Area to meet certain requirements regarding the collection, processing, security and destruction of personal information.

The UK adopted the GDPR requirements and placed them into law with the Data Protection Act 2018. Despite leaving the European Union on 31st December 2020, the UK is committed to meeting the standards of data protection laid down in GDPR and the Data Protection Act 2018. Throughout this policy we will refer to Data Protection Legislation which means GDPR and Data Protection Act 2018 (UK GDPR).

2. Purpose

This policy sets out how The Academy of Gymnastics (The Academy) will seek to ensure compliance with the legislation. The Academy takes its data protection obligations seriously and sets out in this policy how it complies with the various requirements. It covers the way personal information will be obtained, used, shared, physically stored and destroyed.

3. Application

This policy applies to The Academy's dealings with customers and third parties that may be involved in processing customer related information. It covers the way personal information should be obtained, used, shared, physically stored and destroyed.

4. What is personal information?

Personal information relates to an identified or identifiable individual. This could be as simple as a name or a number, however it could include other identifiers such as an email address, physical address, IP address or a mobile phone number.

If it is possible to identify an individual directly from the information held, then that information may be personal information.

Information which has had identifiers removed or replaced in order to pseudonymise the information is still personal data for the purposes of data protection legislation. Information which is truly anonymous is not covered by data protection legislation.

5. The three key elements of Data Protection Legislation

There are 3 key elements of Data Protection Legislation. These three elements then require other conditions to be in place when processing personal information. The three elements are Data Protection Principles, the Rights of the Individual and the Lawful Basis for Processing.

5.1 Data Protection Principles

The General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018 govern the **processing** (i.e., obtaining, holding, organising, recording, retrieval, use, disclosure, transmission, storage, combination and destruction) **of personal and sensitive data** (i.e. information relating to a living individual - the data subject) and sets out the rights of individuals whose information is processed in electronic form or held in a structured paper filing system. There are six principles that describe the legal obligations of organisations that handle personal information about individuals. These Principles are:

1. *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the individual.*
   The information we gather about an individual will be collected in a way where they are fully informed how we intend to use that information, for what purposes and how we will share it.

2. *Personal data shall be 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.*
   We will explain why we need the information we are collecting and will not use it other than for those purposes.

3. *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*
   We will only collect the information we need to provide the services required.

4. *Personal data shall be 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.*
   The information we collect will be accurate and where necessary kept up to date. Inaccurate information will be removed or rectified as we become aware of the changes. We shall request that information is updated by the individual wherever possible.

5. *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; 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 required by data protection legislation in order to safeguard the rights and freedoms of individuals.*
   We will not hold personal information for longer than is necessary.

6. *Personal data shall be 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.

We will make sure that the personal information we have is held securely to ensure that it does not become inadvertently available to other organisations or individuals.

The Academy fully supports these principles.

5.2 Rights of Individuals

Data protection legislation creates specific rights of individuals. These include:

- The right to be informed (about how personal information will be used, shared and stored)
- The right of access (to see a copy of the information held about them)
- The right to rectification (to correct any inaccurate information)
- The right to erasure (to have their personal information removed from our records in certain circumstances)
- The right to restrict processing (to stop the use of their personal information)
- The right to data portability (to take their personal information to another organisation)
- The right to object (to object to the use of their information for marketing purposes)
- Rights in relation to automated decision making and profiling (to understand how automated decision making is used).

5.3 Lawful Basis for Processing

Data Protection Legislation requires that all use of personal information has a lawful basis in place. There are six lawful bases:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

6 What personal information we collect and how we use it

6.1 What we need

The Academy is what's known as the 'Data Controller' of the personal information provided. A Data Controller decides what information is collected, how it is used, how long it is retained and how it will be destroyed. The Academy will collect different types of information depending on the relationship, we usually collect basic personal information such as name, telephone number, address, email address etc.

6.2 Why we need it

The Academy collects personal information in connection with our business activities, such as customer information. We need this information in order to be able to provide our services and expertise to customers.

7. Special Category Information

Special category information is more sensitive, and so needs more protection. Special category information includes information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sexual orientation.

This type of data could create more significant risks to a person's fundamental rights and freedoms, for example, by putting them at risk of unlawful discrimination. In the normal course of business we do not collect all special category information.

8. Handling personal information, lawfully, fairly and transparently

The first and second principles require The Academy to acquire and process personal information lawfully, fairly and in a transparent way. The Academy therefore is clear at the outset about the purpose for which information is obtained and processed. The Academy aims to ensure that:

1. the purpose or purposes for which the information is to be used is made clear to individuals and they have a choice as to whether to provide the information, wherever possible.
2. individuals are provided with easy to read and understand privacy notices when information is collected.
3. personal information is not used in ways that would have adverse effects on individuals.
4. personal information is collected and used only when there are legitimate business reasons which are balanced against the interests of the individual concerned.
5. on request, we can provide to the individual a copy of the personal information we hold about them.
6. personal information will only be handled in ways that individuals would reasonably expect; and
7. there are comprehensive marketing plans and operational procedures in place for initiating contact with prospects and generating sales in a manner that complies with data protection legislation.

Appropriate records will be maintained to demonstrate compliance with the above-mentioned requirements.

9. Consent

Consent will be required for certain types of information usage, generally relating to mailing lists and marketing communications and may be the most appropriate basis for other processing.

When consent is required, it will be freely given, specific, informed and unambiguous. Requests for consent will be separate from other terms and be in clear and plain language. The individuals consent to using their personal data will be as easy to withdraw as to give. Consent must be "explicit" for Special Category Information. The Academy is able to demonstrate that consent was given.

Consent means giving people genuine ongoing choice and control over how you use their data.

Any request for consent will clearly indicate the name of the data controller and the purpose that the information will be used for and how it will be used.

Where explicit consent is required, such as for Special Category information, this consent will be confirmed in words rather than any other positive action.

There is no set time limit for consent and how long it is valid for will depend on the context. Consent will be reviewed and refreshed as appropriate.

Consent requires;

1. the ability to evidence that consent has been provided;

2. that the individual is clear that they have given consent for a specific purpose;

3. the consent to be freely given and not bundled.

10. Contract

Contract as a lawful basis will be relied upon where The Academy process someone's personal data:

- to fulfil contractual obligations to them; or
- because they have asked for something before entering into a contract (e.g., provide a quote) and
- the processing will be necessary.

10.1 When is processing 'necessary' for a contract?

'Necessary' does not mean that the processing must be essential for the purposes of performing a contract or taking relevant pre-contractual steps. Although it should be a relevant and proportionate means of achieving that purpose. If there are other methods that could be used which are less intrusive, they should be applied.

11. Legal Obligation

The Academy will rely on this lawful basis if there is a need to process the personal information in order to comply with a common law or statutory obligation. The specific legal provision or an appropriate source of advice or guidance that clearly sets out the obligation will be used to evidence the legal obligation.

Regulatory requirements also qualify as a legal obligation for these purposes where there is a statutory basis underpinning the regulatory regime and which requires regulated organisations to comply.

12. Vital Interests

12.1 What are 'vital interests'?

Vital interests are only intended to cover events where the processing of personal information is essential to someone's life. It is very limited in scope and usually only applies to matters of life and death.

12.2 When is vital interests likely to apply?

It is usually only relevant to emergency medical care, where you would need to process information about the individual but they may be of incapable of giving consent to the processing at the time. It is unlikely to be used for planned medical care.

13. Public Task

The Public Task basis will cover processing necessary for:

- the administration of justice;
- parliamentary functions;
- statutory functions;
- governmental functions; or
- activities that support or promote democratic engagement.

The underlying legal basis for that function or task is clear and specific.

14. Legitimate Interests

Legitimate interests is the most flexible lawful basis for processing of personal information. It is best used as a lawful basis where the way people's information is used is in a way they would reasonably expect it to be used and which has a minimal impact on their privacy.

There are three elements to using legitimate interests as a basis for processing. These are:

- You need to identify the legitimate interest you plan to use.
- Show that the processing is necessary to achieve it; and
- Then balance this against the individual's interests, rights and freedoms.

The legitimate interests can be our own interests or the interests of third parties and can include commercial interests, individual interests or broader societal benefits.

Wherever legitimate interests is used as the basis for processing, the interests of The Academy will be balanced against those of the individuals whose information is being used.

A legitimate interest assessment will be undertaken to demonstrate compliance and justify the use of personal information.

The Academy may rely on legitimate interests for marketing activities where we have demonstrated that the use of people's data is proportionate, has a minimal privacy impact on the individual and people would not be surprised or likely to object – and where consent is not required under the Privacy and Electronic Communication Regulations (PECR).

15. Fair treatment

Fairness generally requires us to be transparent, i.e. clear at the outset and open with individuals about why the information is being collected and how it will be used. Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair.

The Academy aim to ensure that, in all cases, consent and privacy statements will:

- be clear, fair and not misleading;
- explain the consequences of not providing the required information;
- explain how long the information will be kept for;
- explain if the replies to questions are mandatory or voluntary;
- explain if the information will be transferred overseas;
- explain that if the information will be shared, who with and how they will use it;
- explain how customers may be contacted e.g. telephone, email, SMS, post;
- explain customers' rights – e.g. they can obtain a copy of their personal information;
- explain who to contact if they wish to know more information about how their information is held or to opt-out of receiving further information or if they need to complain; and
- explain customers' right to complain to the Information Commissioner's Office.

The Academy is responsible for ensuring that the following details are communicated to customers:

1. our company name or other trading name as well as the name of any nominated representative where this is appropriate;
2. the purpose(s) for which we intend to process the prospect's or customer's personal information and if the information is to be shared or disclosed to other organisations (so that the individual concerned can choose whether or not to enter into a relationship with the company sharing it);
3. any additional information that will enable us to process the information fairly; and
4. how customers can access the information held about them (as this may help them to spot inaccuracies or omissions in their records – see section below on Rights of Individuals).

16. Minimum amount of personal data

The Academy identify the minimum amount of personal information we need so as to properly fulfil our purpose. We ensure that we hold that much information, but nothing further. If we need to hold particular information about certain individuals, we only collect

the information for those individuals and nothing more. The Academy does not hold personal data on the off chance that it might be useful in the future.

17. Accurate and kept up to date

The Academy will:

- take reasonable steps to ensure the accuracy of any personal information they obtain;
- ensure that the source of any personal information is clear;
- establish if the individual has challenged the accuracy of the information, this is evaluated and recorded carefully; and
- consider whether it is necessary to update the information, particularly if the use of the information relies on the information being current and up to date.

The Academy understands that an expression of an opinion about an individual is classed as their personal information. The record of an opinion (or of the context it is held in) will contain enough information to enable a reader to interpret it correctly. If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, The Academy understand that it is even more important to state the circumstances or the evidence it is based on. Any remarks made in emails or system notes will need to be disclosed if the individual makes a subject access request. Therefore, The Academy ensure that records do not contain anything that might be considered derogatory, or offensive, even though the record may only be for internal use.

18. Marketing

Under the Privacy and Electronic Communication Regulations (PECR) there are specific requirements relating to unsolicited direct marketing communications. A solicited communication is one that is actively invited, either directly by the customer or via a third party. An unsolicited communication is one that the customer has not invited but they have indicated that they do not, for the time being, object to receiving it. If challenged, we would need to demonstrate that an individual has positively opted in to receiving further information from us.

The Academy understands that it is unlawful to contact customers or organisations that have informed us that they do not wish to receive unsolicited marketing material.

19. Children

The Academy provides services which are accessed by children. We obtain the child's information from their parent, guardian, who agrees to provide the information needed for the child to access our services. We ensure that any access and services the child obtains is structured to ensure the privacy of their information and created in a way that is easy for the child to understand.

20. Subject Access Requests

An individual has the right to see the information that The Academy holds about them and can make a request to access this information or receive a copy. Requests may be made verbally or in writing. Requests must be responded to within a calendar month of receipt unless there have been a number of requests or the request is complex, then extra time may be required to respond. The response time can be increased by a further two months, making the maximum response time, three months.

In line with data protection legislation, The Academy will request certain information before responding to a request:

- enough information to judge whether the person making the request is the individual to whom the personal information relates. This avoid personals information about one individual being sent to another, accidentally or as a result of deception.
- Sufficient information that would reasonably be required to find the personal information amongst the records held by us and covered by the request.

In the event of an individual making a subject access request via a third party, for example, a lawyer working on their behalf, The Academy will request written consent from the individual to confirm that the third party can request and receive information on the individual's behalf.

When we respond to a subject access request, we will provide them with the information they are entitled to receive under data protection legislation.

21. Requests for information from law enforcement agencies

Data protection legislation includes exemptions, which allow personal information to be disclosed to law enforcement agencies without the consent of the individual who is the subject of the information, and regardless of the purpose for which the information was originally gathered. The Academy will release personal information to law enforcement agencies if required to do so.

22. Data security

The Academy has appropriate security measures to prevent personal information held being accidentally or deliberately compromised. In particular, The Academy:

- have designed and organised security to fit the nature of the personal information held and the harm that may result from a security breach;
- are clear about everyone's responsibility for ensuring information security;
- make sure that the correct physical and technical security is in place, backed up by robust processes and procedures and reliable, well-trained staff;
- provide regular training to employees so that they may understand their responsibilities; and
- are ready to respond to any breach of security swiftly and effectively.

The Academy recognise that information security breaches may cause real harm and distress to the individuals if their personal information is lost or abused (this is sometimes linked to identity fraud).

23. Managing and monitoring staff

The Academy ensures that staff or those acting on our behalf are aware of, trained and comply with regulatory requirements and company policies on data protection and information security matters.

There are controls in place to ensure that those people handling customer or confidential business information are honest and trustworthy and do not disclose information about customers without checking the identity of contacts and verifying that they are entitled to the information being requested.

There are controls in place to ensure that only authorised personnel can access, alter, disclose or destroy personal information and only act within the scope of their authority. All paper records containing customer information and commercially sensitive information are stored securely when not in use and desks are cleared at the end of the working day.

24. PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) was established by the PCI Security Standards Council to decrease payment card fraud across the internet and increase credit card data security. The Academy comply with the PCI-DSS requirements, this is enforced by the 'acquiring bank' through whom we have our merchant account.
There are twelve key requirements for organisations:

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for passwords or other security parameters.
3. Protect stored data.
4. Encrypt the transmission of cardholder data and sensitive information.
5. Use and regularly update anti-virus software.
6. Develop and maintain securer systems and applications.
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

25. Outsourcing

The Academy have procedures in place if we use third parties to process personal and business information to ensure that we:

- only choose a data processor that provides sufficient guarantees about its security measures to protect the information and the processing it will carry out;
- take reasonable steps to check that those security measures are working effectively in practice; and
- put in place a written contract setting out what the organisation is allowed to do with the personal or business information.

The Academy requires third parties that it works with to ensure that there are adequate security measures in place to secure the information that is being held.

26. Restrictions on transferring information to countries outside the UK and EEA

There are no restrictions on moving personal information from the UK to EEA countries and receiving information. We are open and transparent with our customers and potential customers about where their information is processed and accessed.

On occasion we may need to transfer information outside the UK or EEA and The Academy considers the following factors when deciding whether or not to transfer information overseas:

- the nature of the personal information being transferred;
- how the information will be used and for how long; and
- the laws and practices of the country where information is being transferred to.

We also consider additional factors such as:

- the extent to which the country has adopted data protection standards in its law;
- whether there is a way to make sure the standards are achieved in practice; and
- whether there is an effective procedure for individuals to enforce their rights or get compensation if things go wrong.

If we are unable to gain assurance for the security of the information that it is proposed to transfer, then the transfer will not take place.

27. Data Incidents

The Academy holds, processes, and shares a large amount of personal and business information about customers, contractors and staff. This information needs to be suitably protected. Every care is taken to protect The Academy's information from events and/or incidents (either accidentally or deliberately) to avoid an information security breach that could compromise the security of the information held.

If personal information is accidentally lost, altered or destroyed, attempts to recover it will be made promptly to prevent any damage or distress to the individuals concerned.

The Academy has appropriate security measures in place to prevent personal information held being accidentally or deliberately compromised. In particular, The Academy:

- have designed and organised security to fit the nature of the personal information held and the harm that may result from a security breach;
- are clear about everyone's responsibility for ensuring information security;
- make sure that the correct physical and technical security is in place, backed up by robust processes and procedures and reliable, well-trained staff; and
- are ready to respond to any breach of security swiftly and effectively.

The Academy recognise that information security breaches may cause real harm and distress to the individuals if their personal information is lost or abused (this is sometimes linked to identity fraud).

27.1 Data loss

If personal information is accidentally lost, altered or destroyed, attempts to recover it will be made promptly to prevent any damage or distress to the individuals concerned. In this regard The Academy consider the following:

- containment and recovery – the response to the incident includes a recovery plan and, where necessary, procedures for damage limitation;
- assessing the risks – assess any risks and adverse consequences associated with the breach, as these are likely to affect how the breach needs to be contained;
- notification of breaches – informing the relevant data protection supervisory body as necessary (within 72 hours), law enforcement agencies, data controllers on whose behalf we are working and individuals (whose personal information is affected) about the security breach is an important part of managing the incident.
- evaluation and response – it is important to investigate the causes of the breach, as well as, the effectiveness of controls to prevent future occurrence of similar incidents.

Additionally, The Academy would also look to ensure that any weaknesses highlighted by the information breach are rectified as soon as possible to prevent a recurrence of the incident.

28. Data retention

To comply with information retention best practice, The Academy establish standard retention periods for different categories of information, keeping in mind any professional rules or regulatory requirements that apply and ensuring that those retention periods are being applied in practice. Any personal information that is no longer required will either be archived or deleted in a secure manner.

The Academy's retention periods for different categories of personal information are based on individual business needs.

The Academy understands the difference between permanently deleting a record and archiving it. If a record is archived or stored offline, it will reduce its availability and the risk of misuse or mistake. If it is appropriate to delete a record from a live system, The Academy will also delete the record from any back-up of the information on that system, unless there are business reasons to retain back-ups or compensating controls in place.

29. Secure disposal of records and computer equipment

Once the retention period expires or, if appropriate, the customer or business information is no longer required; paper records will be disposed of in a secure manner. All paper records containing customer or business information are disposed of by shredding. This includes all archived records.

All used computers, mobile phones, printers and any other electronic equipment that may contain or that will have stored customer or business information in electronic format will be disposed of in an appropriate manner after the information has been completely wiped off. An external provider will be used to ensure that the memory on the devices is completely clean of information before the item is disposed of and confirmation of cleansing or destruction obtained.

30. Individual responsibilities

Individuals are responsible for helping The Academy keep their personal information up to date. Individuals should let the company know if information provided changes, for example if you move to a new house or change your bank details.

Staff and contractors may have access to the personal data of staff, freelancers, contractors, customers, suppliers or agents in the course of employment. Where this is the case, The Academy relies on you to help meet our data protection obligations to these individuals.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- to keep data secure (for example by complying with rules on disclosure of data, access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from The Academy's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Unauthorised use, processing or disclosure of personal data (including special categories of personal data), or any serious or deliberate breach of data protection policies or procedures may constitute gross misconduct and could lead to dismissal without notice.

31. Training

The Academy takes its responsibilities with regards to ensuring training is undertaken seriously. We know that having policies and procedures in place provides a solid base for our training programme and we aim to undertake training in accordance with the role and seek specialist advice as and when required. All training is documented and reviewed regularly.

32. Data Protection Impact Assessments (DPIA)

32.1 What is a data protection impact assessment?

Data Protection Impact Assessments or DPIAs are a process to help us identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. By undertaking a DPIA we should be able to identify and fix any data protection issues early.

32.2 When do we need to conduct a DPIA?

We must carry out a DPIA before we process personal information where that processing may result in a high risk to the rights and freedoms of individuals.

Examples of processing that are likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects, or similarly significant effects, on individuals;
- large scale processing of special categories of data or personal data relation to criminal convictions or offences;
- using new technologies (for example surveillance systems).

We will take into account the nature, scope, context and purposes of the processing when deciding whether or not it is likely to result in a high risk to individuals' rights and freedoms.

32.3 What does a DPIA cover?

A DPIA must contain:

- at least a general description of our processing operations and the purposes;
- an assessment of the risks to the rights and freedoms of individuals;
- the measures envisaged to address those risks;
- the safeguards, security measures and mechanisms in place to ensure we protect the personal data; and
- take into account the rights and legitimate interests of the individual's and any other people concerned.

33. Data Protection Officer

Under data protection legislation, you must appoint a DPO if:

- you are a public authority or body (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.

As The Academy does not meet these conditions we have not appointed a Data Protection Officer.

34. Monitoring & Reporting

The manager will monitor the adherence to this policy and report to the other directors any issues or concerns regarding its compliance.

35. Review

This policy will be reviewed periodically in light of changing business priorities and practices and to take into account any changes in legislation.

Updated December 2021