



Introduction

Welcome to Apex1 Studios Limited's privacy policy (Apex1).

Apex 1 respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from) and tell you about your privacy rights and how the law protects you.

You can download a pdf version of the policy here: [LINK](#). Please also use the Glossary to understand the meaning of some of the terms used in this privacy policy.

1. [IMPORTANT INFORMATION AND WHO WE ARE]

2. [THE DATA WE COLLECT ABOUT YOU]

3. [HOW IS YOUR PERSONAL DATA COLLECTED?]

4. [HOW WE USE YOUR PERSONAL DATA]

5. [DISCLOSURES OF YOUR PERSONAL DATA]

6. [INTERNATIONAL TRANSFERS]

7. [DATA SECURITY]

8. [DATA RETENTION]

9. [YOUR LEGAL RIGHTS]

10. [GLOSSARY]

1. Important information and who we are

Purpose of this privacy policy

This privacy policy aims to give you information on how Apex1 collects and processes your personal data through your use of this website, including any data you may provide through this website.

This website is not intended for children and we do not knowingly collect data relating to children.

It is important that you read this privacy policy together with any other privacy policy or fair processing policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy policy supplements other notices and privacy policies and is not intended to override them. Our "Appropriate Policy Document (special categories of personal data)" can be found here.

Controller

Apex1 is the controller and responsible for your personal data ("we", "us" or "our" in this privacy policy).

We have appointed a DPO who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise *our legal rights*, please contact the DPO using the details set out below.

Contact details

If you have any questions about this privacy policy or our privacy practices, please contact our DPO in the following ways:

Full name of legal entity: Apex 1 Studios Limited

Email address: Legal@fit4access.co.uk

Postal address: Bon Marche Centre Unit 201, 241-251 Ferndale Road, London, SW9 8B.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.



Changes to the privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit.

2. The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** includes first name, last name, username or similar identifier, title, age
- **Contact Data** includes billing address, delivery address, email address and telephone numbers.
- **Financial Data** includes bank account and payment card details.
- **Transaction Data** includes details about payments to and from you and other details of services you have purchased from us.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.
- **Profile Data** includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- **Usage Data** includes information about how you use our website, products and services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.
- **Health Data** is collected and used as set out in our Appropriate Policy Document which is set out below.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you, or to facilitate the service being provided to you by our website, and you fail to provide that data when requested, we may not be able to perform service. In this case, we may have to cancel a service you have with us but we will notify you if this is the case at the time.

3. How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Direct interactions.** You give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
 - apply for our products or services;
 - create an account on our website;



- request marketing to be sent to you;
- enter a competition, promotion or survey; or
- give us feedback or contact us.
- **Automated technologies or interactions.** As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. Please see our cookie policy [LINK] for further details.

Technical Data from the following parties:

- (a) analytics providers such as Google based outside the EU;
- (b) Contact, Financial and Transaction Data from providers of technical, payment and delivery services such as Stripe, based inside the EU.

4. How we use your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where you have given us your consent to do so.

We may send you direct marketing communications, and share your data with other third parties who may also contact you about products or services in which you may be interested to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us at consent@fit4access.co.uk.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new user of our service.	(a) Identity (b) Contact (c) Health	(a) Performance of a contract with you; (b) Consent.
To process and deliver your order including: (a) Manage payments, fees and charges; (b) Collect and recover money owed to us.	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing Communications and	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us, marketing)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy;	(a) Identity (b) Contact (c) Profile	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our



(b) Asking you to leave a review or take a survey.	(d) Marketing and Communications	records updated and to study how customers use our products/services)
To enable you to partake in a prize draw, competition or complete a survey.	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you.	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences.	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about goods or services that may be of interest to you.	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and Communications	Necessary for our legitimate interests (to develop our products/services and grow our business)
To allow you to make use of our service on behalf of our Venue Operators.	(a)) health	Details are set out in our Appropriate Policy Document. set out below.



Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or purchased services from us and you have not opted out of receiving that marketing. You may opt out at any time by contacting us at consent@fit4access.co.uk.

Third-party marketing

We may share your contact data with selected third parties whose goods and services we think may be of interest to you.

Opting out

You can ask us or third parties to stop sending you marketing messages at any time by contacting us at any time at consent@fit4access.co.uk.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a product/service purchase, product/service experience or other transactions.

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please see www.fit4access.co.uk/cookiepolicy.pdf

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. Disclosures of your personal data

We may share your personal data with the parties set out below.

- External Third Parties as set out in the [Glossary](#).
- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy policy.



We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

6. International transfers

We do not transfer your personal data outside the European Economic Area (EEA).

OR

[IF TRANSFERS OUT OF EEA OCCUR:] We share your personal data within the [COMPANY] Group. This will involve transferring your data outside the European Economic Area (EEA).]

[IF BINDING CORPORATE RULES ARE USED:] [We ensure your personal data is protected by requiring all our group companies to follow the same rules when processing your personal data. These rules are called "binding corporate rules". For further details, see European Commission: Binding corporate rules.]

[Many of our external third parties are based outside the EEA so their processing of your personal data will involve a transfer of data outside the EEA.]

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented [DELETE AS APPLICABLE]:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between Europe and the US. For further details, see European Commission: EU-US Privacy Shield.



Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

7. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. Data retention

How long will you use my personal data for?

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Details of retention periods for different aspects of your personal data are available in our retention policy which you can request from us by contacting us at legal@fit4access.co.uk.

In some circumstances you can ask us to delete your data: see [your legal rights](#) below for further information.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

9. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. Please click on the links below to find out more about these rights:

- *Request access to your personal data.*
- *Request correction of your personal data.*
- *Request erasure of your personal data.*
- *Object to processing of your personal data.*
- *Request restriction of processing your personal data.*
- *Request transfer of your personal data.*
- *Right to withdraw consent.*

If you wish to exercise any of the rights set out above please contact us at legal@fit4access.co.uk.



No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. Glossary

LAWFUL BASIS

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

THIRD PARTIES

External Third Parties

- Service providers acting as processors based the EEA who provide IT and system administration services. These include Stripe, Inc and ManagedRacks, a division of CSIT Services Ltd
- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers based in the EEA who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities which may include health authorities acting as processors or joint controllers based in the United Kingdom or the Republic of Ireland.
- Third parties who market products and services which we think will be of interest to our users.
- Advisory bodies to professional industries such as UK Active in the sports industry

YOUR LEGAL RIGHTS

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your



personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- If you want us to establish the data's accuracy.
- Where our use of the data is unlawful but you do not want us to erase it.
- Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.
- You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

Appropriate Policy Document: Special Categories of Data

1. About this policy

1.1 This is the "appropriate policy document" for Apex 1 Studios Limited (Apex 1, We) setting out how we will protect Special Categories of Personal Data.

1.2 This policy supports Apex 1 Studios' Data Protection Policy and adopts its definitions.

1.3 This document meets the requirement of the Data Protection Act 2018 that an appropriate policy document be in place where Processing Special Categories of Personal Data in certain circumstances.

2. Definitions

Controller: the person or organisation that determines when, why and how to Process Personal Data.

Data Retention Policy: explains how the organisation classifies and manages the retention and disposal of its information. Time periods for retention are set out in the retention schedule attached to the Data Retention Policy.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

DPA 2018: the Data Protection Act 2018.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the organisation's data privacy team with responsibility for data protection compliance.



GDPR: the General Data Protection Regulation ((EU) 2016/679).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably possess. Personal Data includes Special Categories of Personal Data.

Privacy Policy: a separate notice setting out information that may be provided to Data Subjects when the organisation collects information about them.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

Venue: the physical location of each venue for which the user of www.fit4access.co.uk wishes to gain access, and which is operated by a Venue Operator.

Venue Operator: a party to whom we have entered into a Licence Agreement for the provision of Services through www.fit4access.co.uk

3. Why we process Special Categories of Personal Data

3.1 We process Special Categories of Personal Data for the following purposes:

- (a) Assisting those Venue Operators who use our services through www.fit4access.co.uk to comply with health and safety obligations ;
- (b) Generating a health statement by the user of our service who wishes to enter a Venue, based on information provided by that user, for use by the user and Venue Operator;
- (c) In future we will anticipate government health authorities in sharing data relating to Covid 19 symptoms and location, for example, the NHS test and trace service.

4. Personal data protection principles

4.1 The GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

4.2 We comply with the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

- (a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- (b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
- (d) accurate and where necessary kept up to date (Accuracy);
- (e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation); and
- (f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

4.3 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Compliance with data protection principles

5.1 Lawfulness, fairness and transparency



Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only Process Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. We can Process Special Categories of Personal Data and Criminal Convictions Data only if we have a legal ground for Processing and one of the specific Processing conditions relating to Special Categories of Personal Data or Criminal Convictions Data applies. We will identify and document the legal ground and specific Processing condition relied on for each Processing activity.

When collecting Special Categories of Personal Data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we will provide Data Subjects with a Privacy Notice (above) setting out all the information required by the GDPR in a privacy notice which is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood.

Lawful Processing basis	Processing condition for Special Categories of Personal Data
<p>Data concerning health</p> <p>The Data Subject has consented to the processing of their personal data for one or more specific purposes (Article 6(1)(a))</p>	<p>The Data Subject has given their explicit consent to the processing for one or more specified purposes (Article 2(a));</p>

5.2 Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. They must not be further Processed in any manner incompatible with those purposes.

We will only collect personal data for specified purposes and will inform Data Subjects what those purposes are in a published Privacy Policy. If we use Personal Data for a new compatible purpose, then we will inform the Data Subject first.

5.3 Data minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We will only collect or disclose the minimum Personal Data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the Personal Data collected is adequate and relevant for the intended purposes.

5.4 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the Personal Data we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

5.5 Storage limitation

We only keep Personal Data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once we no longer need Personal Data it shall be deleted or rendered permanently anonymous.

We maintain a Data Retention Policy and related procedures to ensure Personal Data is deleted after a reasonable time has elapsed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

5.6 Security, integrity, confidentiality



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 implement and maintain reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of or damage to Personal Data.

5.7 Accountability principle

We are responsible for, and able to demonstrate compliance with these principles. Our DPO is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the DPO.

We will:

- (a) Ensure that records are kept of all Personal Data Processing activities, and that these are provided to the Information Commissioner on request.
- (b) Carry out a DPIA for any high-risk Personal Data Processing to understand how Processing may affect Data Subjects and consult the Information Commissioner if appropriate.
- (c) Ensure that a DPO is appointed to provide independent advice and monitoring of Personal Data handling, and that the DPO has access to report to the highest management level.
- (d) Have internal processes to ensure that Personal Data is only collected, used or handled in a way that is compliant with data protection law.

6. Controller's policies on retention and erasure of personal data

We take the security of Special Categories of Personal Data and Criminal Convictions Data very seriously. We have administrative, physical and technical safeguards in place to protect Personal Data against unlawful or unauthorised Processing, or accidental loss or damage. We will ensure, where Special Categories of Personal Data or Criminal Convictions Data are Processed that:

- (a) The Processing is recorded, and the record sets out, where possible, a suitable time period for the safe and permanent erasure of the different categories of data in accordance with our Data Retention Policy.
- (b) Where we no longer require Special Categories of Personal Data or Criminal Convictions Data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.
- (c) Where records are destroyed we will ensure that they are safely and permanently disposed of.

Data Subjects receive a Privacy Notice setting out how their Personal Data will be handled when we first obtain their Personal Data, and this will include the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period. The Privacy Notice is also available on our website.

7. Review

7.1 This policy on Processing Special Categories of Personal Data is reviewed regularly.

7.2 The policy will be retained where we process Special Categories of Personal Data and for a period of at least six months after we stop carrying out such processing.

7.3 A copy of this policy will be provided to the Information Commissioner on request and free of charge.

Dated: 13 July 2020

For further information about our compliance with data protection law, please contact our DPO at legal@fit4access.co.uk