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 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**
Data concerning health The Data Subject has consented to the processing of their personal data for one or more specific purposes (Article 6(1)(a))	The Data Subject has given their explicit consent to the processing for one or more specified purposes (Article 2(a));

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