APPROPRIATE POLICY DOCUMENT

Introduction

As part of its operations, it is necessary for Firebrand Training Ltd (Firebrand) to process special category data. Firebrand needs to process personal data about its current and former staff, corporate learners, apprentices, consultants, freelancers and customers to carry out its functions as a provider of corporate training and further education. This policy explains how Firebrand protects special category and criminal offence personal data.

Pursuant to Schedule 1, Part 4 of the DPA 2018, this Appropriate Policy Document explains the processing that may occur and the relevant procedures the Company follows to ensure compliance with data protection legislation and supplements information contained within our privacy notices.

This document should be read in conjunction with Firebrand's data protection policy and privacy notice. This document applies to all employees, including temporary, casual, contract and agency staff, as well as any contractors or service providers acting on behalf of Firebrand, students, suppliers, contractors or consultants, representatives and agents that process or manage personal data on behalf of Firebrand.

1.1. Special category data *(defined by Article 9 of the UK General Data Protection Regulation (GDPR))* and sensitive data *(defined by section 35 of the Data Protection Act 2018 (DPA))* is personal data which reveals:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

1.2. Article 10 GDPR sets out the legal authority for the processing of personal data relating to criminal convictions and offences or related security measures.

1.3. Section 11(2) of the DPA 2018 provides that criminal offence data includes data which relates to the alleged commission of offences and related proceedings and sentencing. Information

about victims and witnesses of crime is also included in the scope of data relating to criminal convictions and offences.

1.4. This policy meets the requirement in the DPA 2018 for an appropriate policy document which details the lawful basis and conditions for processing and safeguards that Firebrand has put in place when processing special category data and criminal offence data.

Description of Data Processed

2.1. Firebrand's Privacy Notice has more information about the information processed by the Company, the legal basis for processing and what the information is used for.

Article 9(1) GDPR prohibits the processing of special categories of data unless at least one condition in Article 9(2) is met. Firebrand must always ensure that its processing is generally lawful, fair and transparent and complies with all the other principles and requirements of the GDPR, which means it will need to identify an Article 6 lawful basis for processing, and, if processing special category data, also an Article 9(2) condition.

2.2. Special Category Data

2.2.1 Firebrand processes special category personal data under the following legal basis:

2.2.1.1 Article 9*(2)(a)* – explicit consent. An example of which would include health information we receive from learners who require additional support.

2.2.1.2 Article 9*(2)(b)* – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on either Firebrand or the data subject in connection with employment, social security, or social protection. For example where Firebrand processes staff sickness and absences information.

2.2.1.3 Article 9*(2)(c)* – where processing is necessary to protect vital interests. An example of this processing would be using health information about a member of staff or learner in a medical emergency.

2.2.1.4 Article 9*(2)(f)* – for the establishment, exercise, or defence of legal claims. Examples of this processing include processing relating to any employment tribunal or other litigation.

2.2.1.6 Article 9*(2)(i)* – where processing is necessary for public health. For example, in relation to Firebrand's processing of data in response to the Covid-19 pandemic.

2.3. Criminal Offence Data

2.3.1 Firebrand processes criminal offence data under Article 10 of the GDPR.

2.3.2 Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Section 10(2) of the DPA 2018 sets out that in order for processing of special categories of personal data to be necessary for the purposes of carrying out the obligations and exercising specific rights of Firebrand or of the data subject in the field of employment, social security and social protection law under Article 9(2)(b) of the UK GDPR, that processing must meet one of the conditions set out in Part 1 of Schedule 1.

Firebrand processes special category data for HR purposes when the condition set out in paragraph 1 of Part 1 of Schedule 1 to the DPA 2018 is met. This condition applies to processing for HR purposes.

Compliance with the Data Protection Principles

3.1 In accordance with the accountability principle, Firebrand maintains records of processing activities under Article 30 of the GDPR and section 61 of the DPA 2018. Firebrand will carry out data protection impact assessments *(where appropriate)* in accordance with Articles 35 and 36 of the GDPR and section 64 of the DPA 2018 to ensure data protection by design and default.

3.2 Firebrand follows the data protection principles set out in Article 5 of the GDPR, and Part 3, Chapter 2 of the DPA 2018 for processing, as follows:

Accountability Principle:

Firebrand has put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to the highest management level.
- Taking a 'data protection by design and default' approach.
- Maintaining documentation of processing activities.
- Adopting and implementing data protection policies.
- Implementing contracts with data processors.
- Implementing appropriate security measures in relation to the personal data.
- Carrying out data protection impact assessments *(where required)*.
- Regular review of accountability measures.

Principle (a): Lawfulness, Fairness, and Transparency

Firebrand provides clear and transparent information about the processing of personal data including the lawful basis for that processing in its Records of Processing Activities (ROPA), Privacy Notice and this policy document.

Principle (b): Purpose Limitation

Where Firebrand shares data with another organisation based on the contractual legal basis (e.g. it's parent or other companies in the BPP Group, it shall document that sharing and do so on the basis of the data sharing agreement in place with the BPP Group.

Firebrand will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): Data Minimisation

Firebrand will only collect personal data necessary for the relevant purposes and ensure it is not excessive. The information processed is necessary for and proportionate.

Where personal data is provided to Firebrand or obtained but is not relevant to our stated purposes, it will be erased.

Principle (d): Accuracy

Firebrand will ensure that where personal data is identified as inaccurate or out of date, having regard to the purpose for which it is being processed, Firebrand will take every reasonable step to ensure that data is erased or rectified without delay. If Firebrand decides not to either erase or rectify it, for example because the lawful basis means those rights don't apply, the decision will be documented.

Principle (e): Storage Limitation

All special category data processed by Firebrand for the purpose of employment or making training adjustments, will only be retained for the periods set out in Firebrand's retention schedule. This retention procedure is reviewed regularly and updated when necessary.

Principle (f): Integrity and Confidentiality (Security)

Firebrand ensures that electronic information is processed within our secure networks and has obtained the Cyber Essentials Plus certification. Hard copy information is processed in line with our security procedures. The systems used to process personal data allow data to be erase or updated as required. Electronic systems and physical storage have appropriate access controls applied.

Further Information

This policy will be retained in accordance with Section 42(3) of the DPA 2018. It will be made available to the ICO on request and reviewed yearly.

The Data Protection Officer can be contacted by email at: DPO@firebrandtraining.com.

Authorisation & Document Control

Document Title	Appropriate Policy Document	**Status**	Live

Classification	Internal and external on request	**Last Review**	October 2023	**Next Review**	October 2024
Location	SharePoint				

Authorisation	**Responsible Person or Body**
Document	Claire Robinson, (external consultant)
Authorised By	BPP Data Protection Team

Version History

Version	Author	Issued	Summary of Changes
1.0	Claire Robinson	August 2022	First APD Document
1.1	Claire Robinson	September 2023	Update to previous APD draft to reflect data sharing within BPP Group.
1.2	Claire Robinson	October 2023	Update to include revisions from BPP legal team.