Data Protection Policy

1. Introduction

This Policy sets out the obligations of Ferfa Limited, a company in England and Wales whose office address is at 9-11 Vittoria Street, Birmingham, England, B1 3ND ("the Company/we/us/our") regarding data protection and the rights of our clients, prospective clients, employees and sub-contractors ("data subjects") in respect of their personal data under the EU General Data Protection Regulation 2016 ("GDPR") and the Data Protection Act 2018 ("DPA").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out in this Policy must be followed at all times by the Company and our employees, sub-contractors, or other parties working on our behalf.

We are committed not only to the letter of the law, but also to the spirit of the law and we place high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom we deal.

The Principles of the GDPR

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR and the DPA. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 **Processed lawfully, fairly, and in a transparent manner** in relation to the data subject.

2.2 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, or for historical research or statistical purposes will not be considered to be incompatible with the initial purposes.

2.3 **Adequate, relevant, and limited** to what is necessary in relation to the purposes for which it is processed.

2.4 **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 it is processed, is erased or rectified without delay.

2.5 Kept in a form which permits **identification of data subjects for no longer than is necessary** for the purposes for which the personal data is 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, or for historical research or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

2.6 **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.

3. The Rights of Data Subjects

3.1 The GDPR sets out the following rights applicable to data subjects (please refer to the relevant parts of this policy for further details):

- 3.1.1 The right to be informed (clause 12).
- 3.1.2 The right of access (clause 13);
- 3.1.3 The right to rectification (clause 14);
- 3.1.4 The right to erasure (also known as the 'right to be forgotten') (clause 15);
- 3.1.5 The right to restrict processing (clause 16);
- 3.1.6 The right to data portability (clause 17);
- 3.1.7 The right to object (clause 18); and
- 3.1.8 Rights with respect to automated decision-making and profiling (clause 19 and 20).

4. Lawful, Fair, and Transparent Data Processing

4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data is lawful if at least one of the following applies:

- 4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;
- 4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- 4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- 4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;
- 4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- 4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

How we deal with data

5. Personal Data We Collect, Hold and Process for Specified, Explicit and Legitimate Purposes

Member Data

5.1 We collect and process the following personal data of the members employees including Member representative, Managing Director, Accounts, Technical, Commercial/Sales, Training, Marketing/PR in order for us to provide our services to our members:

5.1.1 Contact name
5.1.2 Email address;
5.1.3 Phone number;
5.1.4 Postal address;
5.1.5 Site address;
5.1.6 Site and accounts contact details (if different); and
5.1.7 Members References

Prospective Member and Business Contact Data

5.2 We collect and process the following personal data in order for us to respond to enquiries, provide our services and/or where we have received consent to do so:
5.2.1 Contact name;
5.2.2 Email address;
5.2.3 Phone number;
5.2.4 Postal address; and
5.2.5 Site address.

Sub-contractor Data

5.3 We collect and process the following personal data so we can comply with our obligations under the sub-contract and so we can contact and make payments to our sub-contracts:
5.3.1 Name;
5.3.2 Email address;
5.3.3 Phone number;
5.3.4 Postal address;
5.3.5 UTR number; and
5.3.6 Bank details.

Specialised Applied Skills Programme Data

5.4 We collect and process the following personal data so we can comply with our obligations under the programme and so we can contact and ensure we complete our obligations under the contract.
5.4.1 Name;
5.4.2 Email address:
5.4.3 Phone Number;
5.4.4 NI Number;
5.4.5 Employers details; current job role; experience; time in employment;
5.4.6 Qualifications;
5.4.7 Medical History; dietary requirements;

5.5 We only collect, process and hold personal data for the specific purposes set out in this clause 5 of this Policy (or for other purposes expressly permitted by the GDPR).
5.6 We will ensure data subjects are kept informed at all times of the purpose or purposes for which we use their personal data. Please refer to clause 12 for more information on how we keep data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

We will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under clause 5 above.

7. Accuracy of Data and Keeping Data Up to Date

7.1 We will ensure that all personal data collected, processed, and held by us is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in clause 14, below.
7.2 The accuracy of personal data will be checked when it is collected. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.
7.3 We send each member an annual return form to ensure all data we do keep is up to date, it is your responsibility to complete this accurately.

8. Data Retention

8.1 We will not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
8.2 Client contact information will be deleted after 6 years from the date the last contract was completed.
8.3 Sub-contractor personal data will be archived when they leave.
8.4 Prospective member and business contact data will be kept for no longer than 12 months after the last contact is made.
8.5 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
8.6 For full details of our approach to data retention, including retention periods for specific types of personal data we hold, please ask for further information.

9. Secure Processing

We will ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in clauses 21 to 26 of this Policy.

10. Accountability and Record-Keeping

10.1 Our main point of contact for data protection related queries (our "Data Protection Lead") is Mark Spowage, who can be contacted by email at secretariat@ferfa.org.uk.

10.2 Our Data Protection Lead is responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, our other data protection-related policies, and with the GDPR and other applicable data protection legislation.

10.3 We will keep written internal records of all personal data collection, holding, and processing, which will incorporate the following information:

10.3.1 Our Company's name and details, our Data Protection Lead, and any applicable third-party data processors;

10.3.2 The purposes for which we collect, hold and process personal data;

10.3.3 Details of the categories of personal data we collect, hold and process, and the categories of data subject to which that personal data relates;

10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.3.5 Details of how long we will retain the personal data; and

10.3.6 Details of all technical and organisational measures taken by us to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1 We will carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.

11.2 Data Protection Impact Assessments will be overseen by the Data Protection Lead and will address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 Our objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Company; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 We will make the information set out in this clause 12.1 available to every data subject at the time of collection of data:

12.1.1 Our Company's details including, but not limited to, the identity of our Data Protection Lead;

12.1.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in clause 5 of this Policy) and the legal basis justifying that collection and processing;

12.1.3 Where applicable, the legitimate interests upon which we are justifying our collection and processing of the personal data;

12.1.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.1.5 Where the personal data is to be transferred to one or more third parties (such as couriers or payment processing companies), details of those parties;

12.1.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see clause 27 of this Policy for further details);

12.1.7 Details of data retention;

12.1.8 Details of the data subject's rights under the GDPR;

12.1.9 Details of the data subject's right to withdraw their consent to our processing of their personal data at any time;

12.1.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

12.1.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.1.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data we hold about them, what we are doing with that personal data, and why.

13.2 Data subjects wishing to make a SAR should do by emailing our Data Protection Lead using the email address specified in clause 10.1.

13.3 Responses to SARs will normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 All SARs received will be handled by our Data Protection Lead.

13.5 We do not charge a fee for the handling of normal SARs. We reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects have the right to require us to rectify any of their personal data that is inaccurate or incomplete.

14.2 We will rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing us of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that we erase the personal data we hold about them in the following circumstances:

15.1.1 It is no longer necessary for us to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to us holding and processing their personal data;

15.1.3 The data subject objects to us holding and processing their personal data (and there is no overriding legitimate interest to allow us to continue doing so) (see clause 18 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for us to comply with a particular legal obligation.

15.2 Unless we have reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that we cease processing the personal data we hold about them. If a data subject makes such a request, we will retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

We do not use automated means to process personal data.

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to us processing their personal data based on legitimate interests and direct marketing.

18.2 Where a data subject objects to us processing their personal data based on legitimate interests, we will cease such processing immediately, unless it can be demonstrated that our legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to us processing their personal data for direct marketing purposes, we will cease such processing immediately.

19. Automated Decision-Making

We do not use personal data in automated decision-making processes.

20. Profiling

We do not use personal data for profiling purposes.

21. Data Security - Transferring Personal Data and Communications

21.1 All emails containing personal data will be encrypted.

21.2 Personal data will be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

21.3 Where personal data is to be transferred in hardcopy form it will be passed directly to the recipient or sent using normal post.

22. Data Security - Storage

22.1 All electronic copies of personal data are stored securely using passwords and data encryption.

22.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media are stored securely in a locked box, drawer, cabinet, or similar.

22.3 All personal data stored electronically is backed up regularly. Our server backs up data on a daily basis and all back-ups are encrypted.

22.4 Personal data is only stored on mobile devices (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to us or otherwise, with the Data Protection Lead's formal written approval and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

22.5 No personal data will be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to employees, sub-contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to us that all suitable technical and organisational measures have been taken).

23. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it will be securely deleted and disposed of.

24. Data Security - Use of Personal Data

24.1 No personal data may be shared informally and if an employee, sub-contractor or other party working on our behalf requires access to any personal data that they do not already have access to, such access will be formally requested from the Data Protection Lead.

24.2 No personal data may be transferred to any employees, sub-contractors, or other parties, whether such parties are working on our behalf or not, without the authorisation of the Data Protection Lead.

24.3 Personal data must be handled with care at all times and will not be left unattended or on view to unauthorised employees, sub-contractors or other parties at any time.

24.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time,

the user must lock the computer and screen before leaving it.

24.5 Where personal data held by us is used for marketing purposes, it is the responsibility of the Data Protection Lead to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

25. Data Security - IT Security

25.1 All passwords used to protect personal data are changed regularly and are suitably secure in accordance with cyber-security best practice.

25.2 Under no circumstances should any passwords be written down or shared between any employees, sub-contractors or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

25.3 All software (including, but not limited to, applications and operating systems) is kept up to date. Any and all security-related updates must be installed as soon as reasonably and practically possible, unless there are valid technical reasons not to do so.

26. Organisational Measures

26.1 All employees, sub-contractors or other parties working on our behalf and handling personal data are:

- 26.1.1 made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and will be provided with a copy of this Policy;
- 26.1.2 appropriately supervised and trained to do so;
- 26.1.3 required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- 26.1.4 bound to do so in accordance with the principles of the GDPR and this Policy by contract.

26.2 Only employees, sub-contractors or other parties working on our behalf that need access to, and use of, personal data in order to carry out their assigned duties correctly will have access to the personal data held by us.

26.3 Methods of collecting, holding, and processing personal data will be regularly evaluated and reviewed.

26.4 The performance of those employees, sub-contractors or other parties working on our behalf handling personal data will be regularly evaluated and reviewed.

26.5 All sub-contractors or other parties working on our behalf handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of ours arising out of this Policy, the GDPR and the DPA.

26.6 Where any sub-contractor or other party working on our behalf handling personal data fails in their obligations under this Policy, that party shall indemnify and hold us harmless against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

27. Transferring Personal Data to a Country Outside the EEA

27.1 We may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

27.2 The transfer of personal data to a country outside of the EEA will take place only if one or more of the following applies:

- 27.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
- 27.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- 27.2.3 The transfer is made with the informed consent of the relevant data subject(s);
- 27.2.4 The transfer is necessary for the performance of a contract between us and the data subject (or for pre-contractual steps taken at the request of the data subject);
- 27.2.5 The transfer is necessary for important public interest reasons;
- 27.2.6 The transfer is necessary for the conduct of legal claims;
- 27.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- 27.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

28. Data Breach Notification

28.1 All personal data breaches must be reported immediately to our Data Protection Lead.

28.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), our Data Protection Lead will ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

28.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under clause 28.2) to the rights and freedoms of data subjects, our Data Protection Lead will ensure that all affected data subjects are informed of the breach directly and without undue delay.

28.4 Data breach notifications shall include the following information:

- 28.4.1 The categories and approximate number of data subjects concerned;
- 28.4.2 The categories and approximate number of personal data records concerned;
- 28.4.3 The name and contact details of our Data Protection Lead (or other contact point where more information can be obtained);
- 28.4.4 The likely consequences of the breach;

28.4.5 Details of the measures taken, or proposed to be taken, by us to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

29. Implementation of Policy

This Policy shall be deemed effective as of July 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.