DATA RETENTION POLICY

1. This policy sets out the limits for and scope of the retention of personal data and special personal data to ensure that those limits, as well as further data subject rights to erasure, amendment or transfer, are complied with. Furthermore, this policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the General Data Protection Regulation ("GDPR").
2. In addition, this policy also aims to improve the speed and efficiency of managing data.
3. This Policy applies to all personal data held by the Company Intelligent Employment Limited and by third-party data processors processing personal data on the Company's behalf. Personal data, as held by the Company is stored in the following ways and in the following locations:
    a. The Company's servers are located in Wokingham Berkshire.
4. Personal Data means 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, 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.
5. Special Personal Data, or "special category" personal data (also known as "sensitive" personal data) includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.
6. Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).
7. In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:
    a. Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above).
    b. When the data subject withdraws their consent.
    c. When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest.
    d. When the personal data is processed unlawfully (i.e. in breach of the GDPR).
    e. When the personal data must be erased to comply with a legal obligation.
    f. Where the personal data is processed for the provision of information society services to a child.
8. All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection and Data Breach Reporting Policy.
9. Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

10. Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, the right to data portability and further rights relating to automated decision-making and profiling.
11. The Company shall not retain any personal data for any longer than is necessary for the purpose(s) for which that data is collected, held, and processed.
12. Different categories of personal data, used for different purposes, will be retained for different periods and its retention periodically reviewed
13. When considering retention periods, the following shall be considered:
    a. The objectives and requirements of the Company.
    b. The type of personal data in question.
    c. The purpose(s) for which the data in question is collected, held, and processed.
    d. The Company's legal basis for collecting, holding, and processing that data.
    e. The category or categories of data subject to whom the data relates.
14. Under the Conduct of Employment Agencies and Employment Businesses Regulations 2003, the Company is required to keep work-seeker records for at least one year from (a) the date of their creation or (b) after the date on which the Company last provided work-finding services for a work-seeker.
15. The Company must also keep payroll records, holiday pay, sick pay and pensions auto-enrolment records for as long as is legally required by HMRC and associated national minimum wage, social security and tax legislation.
16. If a precise retention period cannot be fixed for a data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.
17. Certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).
18. The following measures are in place within the Company to protect the security of personal data:
    a. All emails containing personal data must be encrypted.
    b. All emails containing personal data must be marked "confidential".
    c. Personal data may only be transmitted over secure networks.
    d. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely.
    e. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it.
    f. All personal data transferred physically should be transferred in a suitable container marked "confidential".
    g. No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the Company's

Data Protection Officer.

h. All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely.

i. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation.

j. Personal data must be handled with care always and should not be left unattended or on view.

k. Computers used to view personal data must always be locked before being left unattended.

l. All electronic copies of personal data should be stored securely using passwords and encryption.

m. All passwords used to protect personal data should be changed regularly and must be secure.

n. Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

o. No software may be installed on any Company-owned computer or device without approval.

p. All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR.

q. Only employees and other parties working on behalf of the Company that need access to, and use of, personal data to perform their work shall have access to personal data held by the Company.

r. All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

s. All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised.

t. All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data always.

u. All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR.

19. Upon the expiry of data retention periods, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of in accordance with the following procedure:

    a. Personal data stored electronically (including all backups thereof) shall be deleted.

    b. Special category personal data stored electronically (including all backups thereof) shall be deleted.

    c. Personal data stored in hardcopy form shall be shredded.

    d. Special category personal data stored in hardcopy form shall be shredded.