

**Suite 1/2 Basepoint**

**Crab Apple Way**

**Evesham**

**WR11 1GP**

**0333 777 8575**

**info@carecheck.co.uk**

**Care Check Terms of Service**

Our client organisations must adhere to the following conditions when applying for, receiving, holding and disposing of Criminal Disclosures via the e-Bulk Online application channel or Paper Route.

1. The Client must nominate a designated individual(s) who will act as the clients contact point for all DBS matters and receive Disclosure information.
2. The client organisation will provide details of the person(s) who will verify the identity of the applicant, and that identity validation will be done in accordance with DBS guidelines using only original documents, and ensure that all applicant details are checked in the same manner.
3. The client organisation must inform Care Check immediately in writing should the person(s) checking the identity of the applicants change.
4. The client organisation will observe and fully adhere to the DBS (CRB) code of practice.
5. The client organisation is likely and will remain likely to genuinely ask an exempted question.
6. The client organisation will make all disclosure applicants aware of the Code of Practice when recruiting and will make a copy available to all disclosure applicants upon request.
7. The client organisation has a satisfactory written policy on the recruitment of ex offenders and issues a copy of the policy to all disclosure applicants at the start of the recruitment process.
8. The client organisation is aware that a statement must be included on its application forms or accompanying documentation, that a disclosure will be requested in the event of an applicant being offered a position.
9. The client organisation is aware that it must include a statement on its application forms, or accompanying documentation, that a criminal record will not necessarily be a bar to obtaining a position.
10. The client organisation must provide a statement in all employment advertisements that Disclosure will be required in the event that a post is offered.
11. The client organisation has a written policy on the secure storage, handling, retention and disposal of disclosure information.
12. The client organisation will not retain disclosures or a record of the information contained within them for longer than is required for the particular purpose. This should be no longer than 6 months after the date on which the recruitment or other relevant decisions have been taken, or after the date on which any dispute about the accuracy of the disclosure information has been resolved. The period should only be exceeded in very exceptional circumstances, which justify retention for a longer period. (Disclosure information may be retained for longer than 6 months for the purpose of audit where organisations are regulated by CQC or OFSTED)
13. All Disclosure certificates will be destroyed in accordance with the DBS (CRB) Code of Practice by shredding, pulping or burning.
14. The client organisation will keep all Disclosure information kept securely, in accordance with the DBS (CRB) Code of practice, separate from their staff members files and within a locked storage unit that cannot be moved by less than 2 persons.
15. The client organisation is aware of what additional information is, and that under no circumstances can this information be divulged to an applicant (or person who is not authorised to have access to this information) and that to do so would constitute a criminal offence.
16. Additional information is very sensitive and must be treated with the utmost caution. Should the client organisation be informed of additional information then they should be careful to base their withdrawal of an offer on employment on pre employment checks, and avoid letting the applicant know that there is “additional information”
17. Client organisations should discuss any matters revealed in the disclosure with the applicant before withdrawing the offer of employment.

Information provided on the disclosure is confidential, and as such should only be available to those persons named in the client contract.

(Unless the person is a registered inspector with the CQC, CSCIW or OFSTED)

1. Care Check reserves the right to make assurance visits to our client organisations to ensure that they are fully complying with the terms and conditions of our contract and the DBS (CRB) Code of Practice.
2. Should Care Check find that any part of this contract is being breached, it reserves the right to withdraw its service with immediate effect.
3. It is the client organisations responsibility to state the level of check they require and if the applicant is working with Children, Vulnerable Adults or both.
4. Care Check shall have no liability for defective services where the defect has been caused or contributed by the client organisation
5. Care Check shall have no liability for defective services where the defect has been caused or contributed by DBS (CRB).
6. Care Check shall have no liability to the client organisation for services if invoice payments have not been received by the due dates of payment.
7. Care Check have no liability for additional damage, loss, liability, claims or expenses caused or contributed to by the Client’s continued use of services or the continued engagement of an Applicant once an error or defect in the relevant Disclosure has become apparent.
8. Care Check shall have no liability for any matters which are outside its reasonable control.
9. Care Check shall have no liability to the client for any consequential losses, loss or profits and/or damage to goodwill, economic losses, special damages and indirect losses or business interruption, loss of business, contracts, opportunity and production.
10. Invoiced Clients shall pay Care Check for all invoices within 15 days of receipt. invoices are raised and sent upon receipt of application. Invoices will be raised for the application if completed correctly or if in need of amendment.
11. Clients using the e-Bulk online channel will ensure that all passwords and log on details are kept private and are under no circumstances passed on to any other person.
12. Clients using the e-Bulk system will change their passwords on a regular basis, preferably every month not rotating the same password within a three month period.
13. Clients using the e-Bulk system shall take reasonable care to ensure that no person is within distance to take note of log on details or disclosure information when accessing the e-Bulk system.
14. ID Checkers using the e-Bulk system shall always check original ID, no photocopies at the time that the information is imputed into the e-Bulk system.
15. Clients using the e-Bulk system shall keep the information held securely on it, unless it needs to be printed for the purposes of audit.
16. Clients using the e-Bulk system who print disclosures for the purpose of audit shall only print them once and shall keep them in accordance with the DBS (CRB) Code of Practice and their policy on the secure storage, retention and disposal of disclosure information.
17. Responsible persons using the e-Bulk system, or the responsible persons Employers shall inform Care Check immediately if they are to leave the client organisation or cease using the system so their log on details can be deleted immediately.
18. ID Checkers, using the e-Bulk system, or the ID Checker employers shall inform Care Check immediately if they are to cease being employed by the client organisation or cease using the system so their log on details can be deleted immediately.
19. Disclosure certificates shall not be passed on to persons not named in the service contract without the written consent of the applicant.

**Care Check Data Processing Agreement/Terms**

**WHEREAS:**

(1) **[**Under a written agreement between the Data Controller and the Data Processor the Data Processor provides tothe Data Controller**]** **OR** **[**The Data Controller from time to time engages the Data Processor to provide tothe Data Controller**]** the Services described in Schedule 1.

(2) The provision of the Services by the Data Processor involves it in processing the Personal Data described in Schedule 2 on behalf of the Data Controller.

(3) Under EU Regulation 2016/679 General Data Protection Regulation (“the GDPR”) (Article 28, paragraph 3), the Data Controller is required to put in place an agreement in writing between the Data Controller and any organisation which processes personal data on its behalf governing the processing of that data.

(4) The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the GDPR in relation to all processing of the Personal Data by the Data Processor for the Data Controller.

(5) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Data Controller by the Data Processor and to all Personal Data held by the Data Processor in relation to all such processing.

**IT IS AGREED** as follows:

1. Definitions and Interpretation
   * 1. In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

|  |  |
| --- | --- |
| **“Data Controller”, “Data Processor”, “processing”, and “data subject”** | shall have the meanings given to the terms “controller”, “processor”, “processing”, and “data subject” respectively in Article 4 of the GDPR; |
| **“ICO”** | means the UK’s supervisory authority, the Information Commissioner’s Office; |
| **“Personal Data”** | means all such “personal data”, as defined in Article 4 of the GDPR, as is, or is to be, processed by the Data Processor on behalf of the Data Controller, as described in Schedule 2; |
| **“Services”** | means those **[**services**] AND/OR [**facilities**]** described in Schedule 1 which are provided by the Data Processor to the Data Controller and which the Data Controller uses for the purpose**[**s**]** described in Schedule 1; |
| **“Sub-Processor”** | means a sub-processor appointed by the Data Processor to process the Personal Data; and |
| **“Sub-Processing Agreement”** | means an agreement between the Data Processor and a Sub-Processor governing the Personal Data processing carried out by the Sub-Processor, as described in Clause 10. |

* + 1. Unless the context otherwise requires, each reference in this Agreement to:
       - 1. “writing”, and any cognate expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;
         2. a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;
         3. “this Agreement” is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;
         4. a Schedule is a schedule to this Agreement; and
         5. a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule.
         6. a "Party" or the "Parties" refer to the parties to this Agreement.
    2. The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.
    3. Words imparting the singular number shall include the plural and vice versa.
    4. References to any gender shall include all other genders.
    5. References to persons shall include corporations.

1. Scope and Application of this Agreement
   * 1. The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 2, carried out for the Data Controller by the Data Processor, and to all Personal Data held by the Data Processor in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.
     2. The provisions of this Agreement supersede any other arrangement, understanding, or agreement **[**including, but not limited to, the Service Agreement**]** made between the Parties at any time relating to the Personal Data.
     3. This Agreement shall continue in full force and effect for so long as the Data Processor is processing Personal Data on behalf of the Data Controller, and thereafter as provided in Clause 9.
2. Provision of the Services and Processing Personal Data

The Data Processor is only to carry out the Services, and only to process the Personal Data received from the Data Controller:

* + 1. for the purposes of those Services and not for any other purpose;
    2. to the extent and in such a manner as is necessary for those purposes; and
    3. strictly in accordance with the express written authorisation and instructions of the Data Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Data Controller to the Data Processor).

1. Data Protection Compliance
   * 1. All instructions given by the Data Controller to the Data Processor shall be made in writing and shall at all times be in compliance with the GDPRand other applicable laws. The Data Processor shall act only on such written instructions from the Data Controller unless the Data Processor is required by law to do otherwise (as per Article 29 of the GDPR).
     2. The Data Processor shall promptly comply with any request from the Data Controller requiring the Data Processor to amend, transfer, delete, or otherwise dispose of the Personal Data.
     3. The Data Processor shall transfer all Personal Data to the Data Controller on the Data Controller’s request in the formats, at the times, and in compliance with the Data Controller’s written instructions.
     4. Both Parties shall comply at all times with the GDPR and other applicable laws and shall not perform their obligations under this Agreement or any other agreement or arrangement between themselves in such way as to cause either Party to breach any of its applicable obligations under the GDPR.
     5. The Data Controller hereby warrants, represents, and undertakes that the Personal Data shall comply with the GDPR in all respects including, but not limited to, its collection, holding, and processing, and that the Data Controller has in place all necessary and appropriate consents and notices to enable the lawful transfer of the Personal Data to the Data Processor.
     6. The Data Processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with any and all applicable legislation from time to time in force (including, but not limited to, the GDPR) and any best practice guidance issued by the ICO.
     7. The Data Processor shall provide all reasonable assistance **[**(at the Data Controller’s cost)**]** to the Data Controller in complying with its obligations under the GDPR with respect to the security of processing, the notification of personal data breaches, the conduct of data protection impact assessments, and in dealings with the ICO.
     8. When processing the Personal Data on behalf of the Data Controller, the Data Processor shall:
        + 1. not process the Personal Data outside the **[**United Kingdom**] OR [**European Economic Area (all EU member states, plus Iceland, Liechtenstein, and Norway) (“EEA”)**]** without the prior written consent of the Data Controller and, where the Data Controller consents to such a transfer to a country that is outside of the EEA, to comply with the obligations of Data Processors under the provisions applicable to transfers of Personal Data to third countries set out in Chapter 5 of the GDPR by providing an adequate level of protection to any Personal Data that is transferred;
          2. not transfer any of the Personal Data to any third party without the written consent of the Data Controller and, in the event of such consent, the Personal Data shall be transferred strictly subject to the terms of a suitable agreement, as set out in Clause 10;
          3. process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Data Controller or as may be required by law (in which case, the Data Processor shall inform the Data Controller of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law);
          4. implement appropriate technical and organisational measures, as described in Schedule 3, and take all steps necessary to protect the Personal Data against unauthorised or unlawful processing, accidental loss, destruction, damage, alteration, or disclosure. The Data Processor shall inform the Data Controller in advance of any changes to such measures;
          5. if so requested by the Data Controller (and within the timescales required by the Data Controller) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;
          6. keep complete and accurate records and information concerning all processing activities carried out on the Personal Data in order to demonstrate its compliance with this Agreement;
          7. make available to the Data Controller any and all such information as is reasonably required and necessary to demonstrate the Data Processor’s compliance with the GDPR;
          8. on **[**at least 30 days'**]** **OR** **[**reasonable**]** prior notice, submit to audits and inspections and provide the Data Controller with any information reasonably required in order to assess and verify compliance with the provisions of this Agreement and both Parties’ compliance with the requirements of the GDPR. The requirement to give notice will not apply if the Data Controller believes that the Data Processor is in breach of any of its obligations under this Agreement or under the law; and
          9. inform the Data Controller immediately if it is asked to do anything that infringes the GDPR or any other applicable data protection legislation.
2. Data Subject Access, Complaints, and Breaches
   * 1. The Data Processor shall **[**, at the Data Controller’s cost,**]** assist the Data Controller in complying with its obligations under the GDPR. In particular, the following shall apply to data subject access requests, complaints, and data breaches.
     2. The Data Processor shall notify the Data Controller **[**without undue delay**] OR** **[**within30 days**]** if it receives:
        + 1. a subject access request from a data subject; or
          2. any other complaint or request relating to the processing of the Personal Data.
     3. The Data Processor shall **[**, at the Data Controller’s cost,**]** cooperate fully with the Data Controller and assist as required in relation to any subject access request, complaint, or other request, including by:
        + 1. providing the Data Controller with full details of the complaint or request;
          2. providing the necessary information and assistance in order to comply with a subject access request;
          3. providing the Data Controller with any Personal Data it holds in relation to a data subject (within the timescales required by the Data Controller); and
          4. providing the Data Controller with any other information requested by the Data Controller.
     4. The Data Processor shall notify the Data Controller immediately if it becomes aware of any form of Personal Data breach, including any unauthorised or unlawful processing, loss of, damage to, or destruction of any of the Personal Data.
3. [Appointment of a Data Protection Officer
   * 1. **[**The Data Controller has appointed a Data Protection Officer in accordance with Article 37 of the GDPR
     2. **[**The Data Processor shall appoint a Data Protection Officer in accordance with Article 37 of the GDPR and shall supply the details of the Data Protection Officer to the Data Controller prior to the commencement of the processing.**]**  
          
        **OR**  
          
        **[**The Data Processor has appointed a Data Protection Officer in accordance with Article 37 of the GDPR
4. Liability and Indemnity
   * 1. The Data Controller shall be liable for, and shall indemnify (and keep indemnified) the Data Processor in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Data Processor **[**and any Sub-Processor**]** arising directly or in connection with:
        + 1. any non-compliance by the Data Controller with the GDPR or other applicable legislation;
          2. any Personal Data processing carried out by the Data Processor **[**or Sub-Processor**]** in accordance with instructions given by the Data Controller that infringe the GDPR or other applicable legislation; or
          3. any breach by the Data Controller of its obligations under this Agreement,

except to the extent that the Data Processor **[**or Sub-Processor**]** is liable under sub-Clause 7.2.

* + 1. The Data Processor shall be liable for, and shall indemnify (and keep indemnified) the Data Controller in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Data Controller arising directly or in connection with the Data Processor’s Personal Data processing activities that are subject to this Agreement:
       - 1. only to the extent that the same results from the Data Processor’s **[**or a Sub-Processor’s**]** breach of this Agreement; and
         2. not to the extent that the same is or are contributed to by any breach of this Agreement by the Data Controller.
    2. The Data Controller shall not be entitled to claim back from the Data Processor **[**or Sub-Processor**]** any sums paid in compensation by the Data Controller in respect of any damage to the extent that the Data Controller is liable to indemnify the Data Processor **[**or Sub-Processor**]** under sub-Clause 7.1.
    3. Nothing in this Agreement (and in particular, this Clause 7) shall relieve either Party of, or otherwise affect, the liability of either Party to any data subject, or for any other breach of that Party’s direct obligations under the GDPR. Furthermore, the Data Processor hereby acknowledges that it shall remain subject to the authority of the ICO and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a data processor under the GDPR may render it subject to the fines, penalties, and compensation requirements set out in the GDPR.

1. Intellectual Property Rights

All copyright, database rights, and other intellectual property rights subsisting in the Personal Data (including but not limited to any updates, amendments, or adaptations to the Personal Data made by either the Data Controller or the Data Processor) shall belong to the Data Controller or to any other applicable third party from whom the Data Controller has obtained the Personal Data under licence (including, but not limited to, data subjects, where applicable). The Data Processor is licensed to use such Personal Data under such rights only **[**for the term of the Service Agreement,**]** for the purposes of the Services, and in accordance with this Agreement.

1. Confidentiality
   * 1. The Data Processor shall maintain the Personal Data in confidence, and in particular, unless the Data Controller has given written consent for the Data Processor to do so, the Data Processor shall not disclose any Personal Data supplied to the Data Processor by, for, or on behalf of, the Data Controller to any third party. The Data Processor shall not process or make any use of any Personal Data supplied to it by the Data Controller otherwise than in connection with the provision of the Services to the Data Controller.
     2. The Data Processor shall ensure that all personnel who are to access and/or process any of the Personal Data are contractually obliged to keep the Personal Data confidential.
     3. The obligations set out in in this Clause 9 shall continue for a period of 30 days after the cessation of the provision of Services by the Data Processor to the Data Controller.
     4. Nothing in this Agreement shall prevent either Party from complying with any requirement to disclose Personal Data where such disclosure is required by law. In such cases, the Party required to disclose shall notify the other Party of the disclosure requirements prior to disclosure, unless such notification is prohibited by law.
2. Appointment of Sub-Processors
   * 1. The Data Processor shall not sub-contract any of its obligations or rights under this Agreement without the prior written consent of the Data Controller (such consent not to be unreasonably withheld).
     2. In the event that the Data Processor appoints a Sub-Processor (with the written consent of the Data Controller), the Data Processor shall:
        + 1. enter into a Sub-Processing Agreement with the Sub-Processor which shall impose upon the Sub-Processor the same obligations as are imposed upon the Data Processor by this Agreement and which shall permit both the Data Processor and the Data Controller to enforce those obligations; and
          2. ensure that the Sub-Processor complies fully with its obligations under the Sub-Processing Agreement and the GDPR.
     3. In the event that a Sub-Processor fails to meet its obligations under any Sub-Processing Agreement, the Data Processor shall remain fully liable to the Data Controller for failing to meet its obligations under this Agreement.
3. Deletion and/or Disposal of Personal Data
   * 1. The Data Processor shall, at the written request of the Data Controller, delete (or otherwise dispose of) the Personal Data or return it to the Data Controller in the format(s) reasonably requested by the Data Controller within a reasonable time after the earlier of the following:
        + 1. the end of the provision of the Services **[**under the Service Agreement**]**; or
          2. the processing of that Personal Data by the Data Processor is no longer required for the performance of the Data Processor’s obligations under **[**this Agreement**] AND/OR [**the Service Agreement**]**.
     2. Following the deletion, disposal, or return of the Personal Data under sub-Clause 11.1, the Data Processor shall delete (or otherwise dispose of) all further copies of the Personal Data that it holds, unless retention of such copies is required by law, in which case the Data Processor shall inform the Data Controller of such requirement(s) in writing.
     3. All Personal Data to be deleted or disposed of under this Agreement shall be deleted or disposed of using the following method(s): Data Cleanse via system.
4. Law and Jurisdiction
   * 1. This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.
     2. Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.