CSAS e-Bulk End User Agreement

For Disclosure and Barring Checking Services

Where authorised users receive the managed online service via the Catholic Safeguarding Advisory Service (CSAS) e-Registered Body, the following provisions shall apply in accordance with the CSAS Procedures Manual Safer Recruitment Practice guidance, particularly the CSAS Information Security Policy, and with adherence to the Disclosure and Barring Service (DBS) Code of Practice and Data Protection Act 1998.

4.2 Safer Recruitment Practice Including DBS Disclosures
http://www.csasprocedures.uk.net/chapters/p_safer_recruit.html#obligations

1. User Obligations

1.1. The user agrees to:

a) Ensure that each applicant completes all mandatory details on the application form. The user shall procure that its nominated representative(s) check each application form for accuracy and completeness prior to submission and will verify each applicant's identification documents in accordance with the user's obligations under this agreement.

b) Submit all completed and checked application forms via the managed service for provision of the services in relation to such application forms.

c) Ensure that the position of the applicant entitles them to the check as per the requirements of the government agency. By requesting the check on the applicant, the user agrees that the job position of the applicant meets the relevant government agency eligibility requirements.

d) Ensure application forms are completed fully and proof of the applicant's identity has been provided as per government agency guidelines and codes of practice. Failure to do so will void the application form.

e) Ensure that all volunteer application forms submitted meet the government agency requirements for a volunteer.

f) Use and apply the information solely for the purpose of submitting the application forms and receiving the Disclosures/Disclosure information.

g) Ensure E-Bulk schema results are not printed out, nor retained electronically other than within the e-Bulk system.

h) Ensure that services are only accessed by authorised users.

i) Ensure that application forms are not submitted for personal reasons or provided to any third party unless expressly permitted by prior agreement with CSAS.

j) Be responsible for:

i. Obtaining the informed express written consent (permission) of the relevant individuals prior to the relevant services being performed.

ii. Complying with its obligations under this agreement including but not limited to the obligations in relation to obtaining express consent of applicants.

k) Acknowledge that CSAS holds no responsibility for any issue of liability arising from use of the user's or applicant's equipment.

2. Operating Procedures/Access Rights

2.1. Only named individuals/users are provided access to the e-Bulk system and are allocated specific roles. These are Master Disclosure Manager, Disclosure Manager, ID Verifier, Counter Signatory and Administrator. E-Bulk user passwords will be provided following training and the signing of this agreement.

2.2. The **Master Disclosure Manager** is responsible for:

a) Creating a Disclosure Manager
b) Creating an ID Verifier
c) Creating an Applicant
d) Viewing the outcome of the check and associated letters
e) Exporting information.

2.3. The **Disclosure Manager** is responsible for:

a) Creating an ID Verifier
b) Creating an Applicant
c) Viewing the outcome of the check and associated letters
d) Exporting information.

2.4. The **Countersignatory** is responsible for:

a) Creating an ID Verifier
b) Creating an Applicant
c) Exporting information.
d) Creating a appear application (which also Verifies the application)
e) Creating organisations
f) Countersigning an application

2.5. The **Administrator** is responsible for:

a) Creating an ID Verifier
b) Creating an Applicant
c) Exporting information.
d) Creating a appear application (which also Verifies the application)
e) Creating organisations

2.6. The **ID Verifier** is responsible for:

a) Creating an Applicant
b) Verifying Applicant identity.

2.7. All users must:

a) Ensure passwords are kept strictly confidential, with no Disclosure or unauthorised use of passwords or sharing between users.
b) Not access the services via any unsecured wireless hand-held communication device and/or personal computers and/or removable data storage equipment or media to store any information relating to the managed service.

2.8. Master Disclosure Managers/Disclosure Managers/Counter Signatories/Administrators must:

a) Ensure all workstations, devices and servers used to access the managed service are placed in a secure location, are secured when not in use through such means as locked

screens, shutting power controls off, in a restricted environment or other reasonable security procedures.

b) Ensure all workstations, devices and servers used to access the system have appropriate up to date anti-virus software, anti-malware and an active firewall.

3. Termination

3.1. Upon termination of a user's employment:

a) CSAS Head Office will revoke Master Disclosure Manager access to the system.

b) The Master Disclosure Manager is responsible for revoking all Disclosure Manager and ID Verifier access to the system for their organisation.

c) The Master Disclosure Manager should ensure the CSAS DBS Exit Form is completed upon de-registering a user from the system.

3.2. Upon termination of this agreement for any reason:

a) Any application forms that are unprocessed at the date of termination will be returned to the user.

b) The user shall not submit any further application forms and the service provider will not accept any further submissions from the user.

4. CSAS Obligations

4.1. Completed, checked and countersigned application forms submitted via the managed service will be submitted to the DBS for processing.

4.2. In the event of a clear Disclosure, the appropriate authorised user will be notified of the fact that the Disclosure is clear via the service provider. Alternatively this information may be viewed via an online report.

4.3. Where there is a blemished Disclosure, the appropriate authorised user will be notified that the Disclosure has content and the user should submit a request to the applicant to have sight of the Disclosure.

4.4. The user shall be notified as soon as reasonably practical if a Disclosure may be incorrect or incomplete.

5. CSAS Security Obligations

5.1. If a security incident occurs, CSAS shall carry out an immediate investigation.

5.2. If CSAS becomes aware of any data security contravention, security incidents or any unauthorised access by its personnel or other connected parties, CSAS shall:

a) Report such incidents to the service provider immediately.

b) Describe in full detail any accessed material.

c) Return to the service provider any copied or removed material.

d) Comply with all directions and requests made by the service provider.

6. Audit Rights

6.1. Where the DBS has exercised its right of audit under its agreement with CSAS, users shall cooperate with CSAS's requests allowing access to the user's records or sites as required to enable compliance with the DBS.

7. Business Continuity

7.1. If the e-Bulk service is rendered unavailable for a period of 5 or more working days then CSAS shall revert to the paper process.

Signature ……..

Full Name (capitals): ……..

Role (please tick relevant box below):

- ☐ Master Disclosure Manager
- ☐ Countersignatory
- ☐ Ebulk Administrator
- ☐ Disclosure Manager
- ☐ ID Verifier

Other (please state) ……..

Organisation: ……..

Date: ……..

Please retain a copy of this agreement for your reference.