Disclosure &
Barring Service

# E-BULK
# INTERCHANGE AGREEMENT

## Version 9.0

Date: 10th February 2017

# Contents

Table of Contents

# 1 Introduction

This Interchange Agreement represents a binding agreement between the DBS and e-Bulk-enabled RBs with respect to the DBS's e-Bulk service. This document is referenced by the Memorandum of Understanding [9] or Deed [10]. See section 1.2.

## 1.1 Background

The DBS's "e-Bulk" interface is a facility to enable applications for DBS checks to be bulk-submitted electronically and to return information regarding the results by a similar means.

Registered Bodies (RBs) who wish to use the e-Bulk facility may register to do so providing they meet DBS's criteria. RBs that have registered for e-Bulk are referred to as e-RBs.

Use of the e-Bulk interface alleviates the need for the production and mailing of paper forms by e-RBs and form scanning, and data keying by the DBS.

.

## 1.2 Purpose of the document

The purpose of this document is to define and document the agreement between the DBS and e-Bulk-enabled RBs with respect to each e-RB's use of, and the DBS's provision of, the e-Bulk service.

The agreement captures the responsibilities and requirements of these parties with respect to the exchange of information over the e-Bulk interface. Within this, it highlights how pre-existing responsibilities, including those embodied in the DBS Code of Practice [8] and the Data Protection Act 1998, extend to use of the e-Bulk service. Where appropriate, it summarises these responsibilities and requirements and makes reference to other documents to provide details.

For public sector RBs a Memorandum of Understanding (MoU) that references the text of this agreement is provided as a separate document. The MoU has been approved by the Home Office. For private sector RBs an e-Bulk Deed which is a legally binding document that references the text of this agreement is provided as a separate document. To participate in the e-Bulk initiative, Registered Bodies will need to agree to the conditions set out therein. Both the MoU and the Deed set out the terms of the relationship between the parties and the proposed action in the event of a breach of that agreement. The MoU or e-Bulk Deed must be signed by the Lead Signatory of the RB.

## 1.3 Scope

The scope of this document is the agreement between an e-RB and the DBS with respect to the e-RB's use of the live e-Bulk service made available by the DBS. It applies specifically in respect of the e-RB's use of the e-Bulk service once they have been enabled on the live e-Bulk service, rather than during the provisioning process in which an RB works with the DBS in preparation for becoming an e-RB. Nevertheless, in preparing to use the service, each RB will have to develop their solution for connecting to the e-Bulk service in such a way that it complies with the requirements set out herein.

## 1.4 References

The table below lists references to other relevant e-Bulk documentation. References to these documents, if and when included within the text of this document, are made using the square-bracket notation shown in the "Ref" column of the table.

| Ref | Details |
|---|---|
| [1] | e-Bulk  Business Process Document |
| [2] | e-Bulk Business Message Specification |
| [3] | e-Bulk Message Integrity Specification |
| [4] | Interface Control Document : ICD DBS Managed File Transfer Service for eBulk |
| [5] | Document removed details incorporated in [4] |
| [6] | Canopy Digital Connect Code of Connection |
| [7] | CDC MFTS Onboarding for DBS |
| [8] | Code of Practice and Explanatory Guide for Registered Persons and other recipients of Disclosure Information DBS05-12/2001 |
| [9] | Memorandum of Understanding |
| [10] | Deed |

## 1.5 Abbreviations & Terminology

This section provides definitions of abbreviations and unusual terminology used in this document.

### Abbreviations

| Abbreviation | Meaning |
|---|---|
| CDC | Canopy Digital Connect, a configurable 'Software as a Service' (SaaS) messaging solution provided by Atos that enables the secure exchange of messages and data between disparate government and non- government IT systems connected via the internet and the Public Services Network (PSN). |
| DBS | Disclosure and Barring Service |
| e-RB | An RB that is registered and enabled for use of the e-Bulk service |
| FTP | File Transfer Protocol: a protocol for transferring data between computers across a network |
| FTPS | FTP secured with TLSFTP over SSL: a variant to FTP that uses secure communications over SSL or TLS |
| HMG | Her Majesty's Government |
| PSN | Public Service Network is the UK government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources. See https://www.gov.uk/government/groups/public-services-network |
| RB | Registered Body |
| TLS | Transport Layer Security. A cryptographic protocol that provides secure communications over a computer network. |
| TCS | Tata Consultancy Service (DBS Private Sector partner) |
| XML | eXtensible Markup Language |

## Terminology

| Term | Meaning |
|---|---|
| 3rd Party | In DBS e-bulk service terms a 3rd party is any organisation or individual other than the RB who has access to DBS electronic application data either on a continual or ad hoc basis. (If a 3rd party supplier/data processor develops an e-bulk system but then no longer has access to the software, hardware or data once the RB is live on the e-bulk service then this does not constitute using a 3rd party). |
| Business Assurance Gate | (BAG) a natural extension of the existing RB assurance function confirming the e-RB has sufficient business processes in place to carry out Disclosure applications using the e-Bulk interface in accordance with DBS requirements. |
| e-Bulk | The term that has been given to the interface described in this document, named as such because it provides an electronic mechanism for submitting applications in bulk (i.e. in batches, as opposed to one at a time). This is analogous to the current practice of sending paper DBS applications in bulk by post. In some cases, it may also be written as "eBulk" |
| eBulk Application | An application for a DBS check sent by electronic means. In the context of this document, this refers to a DBS application sent via the e-Bulk interface. |
| eBulk Result | An electronically delivered response to an e-Bulk Application. An e-Bulk Result indicates to an RB, either that the result of the DBS check is 'blank' or that the RB should wait to view the applicant's certificate. |
| ISO27001 | An ISO standard for information security management ( http://www.iso.org/iso/iso27001 |
| Malware | Malicious software; software designed to infiltrate or damage a computer system. |
| Technical Assurance Gate | (TAG) will prove the technical compatibility and robustness of each e-RB system as part of the on-boarding process. |
| XML Schema | A standard for defining the format of XML documents. The standard provides a means by which tools can know the correct format of a document, enabling them to provide generic operations such as validation. |

# 2 Information Security, Data Protection & Code of Practice

This section is concerned with the responsibilities of all parties with respect to the protection and proper handling of the information exchanged over e-Bulk and the protection of the infrastructure underpinning it.

## 2.1 Information Classification

The information that passes over the e-Bulk interface is classed as sensitive personal data covered by the Data Protection Act 1998. This includes details provided as part of applications for DBS Checks and the corresponding acknowledgements and responses that are returned. All parties must, therefore, ensure that this information is handled in accordance with their respective responsibilities under this Act.

UK Government organisations using the e-Bulk interface may wish to note that the information that passes over the e-Bulk interface has been classified as Official - Sensitive during transmission between RBs and the DBS (Details relating to the current Government security classifications can be found at https://www.gov.uk/government/publications/government-security-classifications).

## 2.2 Security Requirements

The DBS Code of Practice [8] places responsibilities on Registered Bodies to correctly handle and safeguard information. These responsibilities extend to the use of the e-Bulk service and the IT systems that interface with it, in accordance with the information classification noted above.

Users of the e-Bulk service must have a written security policy, which must be reviewed and, where necessary, updated to ensure that it adequately addresses electronic processing and communication of data introduced by use of the e-Bulk service, in order to meet these responsibilities. A copy of the policy must be made available on request to the DBS during the Business Assurance Gateway review 6.6.
Areas that the security policy will need to consider include:

- The sensitivity classification of information gathered, stored and exchanged.
- How data will be handled, stored, transmitted, deleted and destroyed.
- How responsibilities under the Data Protection Act 1998 will be met.
- Who has access to data ,including 3rd parties/suppliers/data processors,
- How that access, both electronic and physical, is authorised within the organisation, and audited 'Access' would include external access to the system for the purposes of maintenance or upgrade
- The handling of technical information such as FTP passwords, digital certificates and cryptographic material.

An approach that is compliant with ISO27001 is considered as best practice in this area. It is therefore a requirement for the RB's connection to the e-Bulk service that their Information Security Management Systems are certified or compliant to ISO 27001 and this should be verified by an independent assessment/audit. This also applies to any 3rd Parties, Suppliers/data processors with access to data.

The DBS and other parties involved in the provision of the e-Bulk service have similar responsibilities to correctly handle and safeguard information exchanged over the e-Bulk interface. The RB is responsible for information on the data path into the DBS but not on the way out as DBS retains responsibility for the information at that point.

### 2.2.1 Restricted Correspondence

E-RBs are reminded that all information with a marking of Official must not be sent via a non secure email address and nothing above Official should be transmitted. Two individuals in each prospective e-RB will be set up with a Criminal Justice Secure e-Mail facility that must be used for communicating any information classified as Restricted or Official (Details relating to the current Government security classifications can be found at https://www.gov.uk/government/publications/government-security-classifications). The individuals set up with the CJSM account will be provided with instructions on its use and will adhere to and sign a copy of the terms and conditions.

### 2.2.2 Message Integrity

The e-Bulk service includes facilities to protect the integrity of each message during transmission between the end points of the interface. These facilities are included to ensure that data cannot change during transmission without being detected.

DBS and e-RB responsibilities related to processing of messages are described in section 5.4. These include the investigation/reporting of failed integrity checks. There are additional security responsibilities related to message integrity protection, and these are described here in this section.

TCS on behalf of DBS will
i.) Issue message integrity protection keys [3] to e-RBs and in conjunction with the e-RB will manage expiry and renewal of these keys. It is advisable for the e-RB to take note of expiry dates of integrity keys for their records. If the integrity key were to expire the RB would no longer be able to successfully send or receive e-Bulk messages.

ii.) Take measures, in accordance with HMG best practice, to ensure that the message integrity keys that it holds are held securely and protected from compromise.

e-RBs must
i.) Take measures to hold message integrity keys securely, in order to prevent their compromise, in accordance with the best practices recommended by ISO27001:2013 section A.12.3.

ii.) Report any compromise or potential compromise of integrity keys as a security incident as soon as possible, according to section 7.6.

iii.) Destroy all copies of expired and revoked integrity keys as soon as possible after expiry or revocation.

iv.) Have an individual, nominated by the Lead Signatory, to be directly responsible for all aspects of key management and key accounting. The details of the individual will be recorded in the MoU [9] or e-Bulk Deed [10]. That individual must be aware of their responsibilities and be adequately trained. Note that in the case of an RB using the services of a DBS approved 3rd Party, this role may be assigned to a nominated person within the 3rd Party. Protective measures should be in place to ensure integrity keys are not disclosed to or accessible to unauthorised persons. An audit trail must record all instances of access to keys and their associated information and this should be kept for 6 months.

v.) Have a process to apply new integrity keys in place of expiring integrity keys at a specific date and time (which will typically be the time of expiry of the expiring key). This process must ensure that the sending of messages using the expiring key is stopped at 18:00 hours on the day the key expires and that new messages are not sent until after 12:00 hours on the day the new key becomes valid. The e-RB must ensure before changing the key that any files received from the DBS on that day have been processed. This is to minimise the risk that messages sent with an expiring key will be received and processed after that key has expired; the process must allow for the fact that any failures as a result of this will be dealt with by manual workaround.

vi.) Have a process to ensure that, when any member of staff who has access to integrity keys leaves the RB organisation or no longer has authorisation to access integrity keys, the integrity key(s) to which the staff member has had access are revoked and a new key (to which the staff member will not have access) is issued by the DBS. The revocation and new key request should be raised as a security incident to the DBS according to the procedures described in 7.6.

vii.) Have a process to inform DBS First Line Support of a change of the individual responsible for Key Management.

### 2.2.3 Compliance with Atos Canopy Digital Connect (CDC) Security Policy

All systems, interfaces and processes involved in the interchange of messages over the e-Bulk interface shall be the subject of an appropriate information security policy, sufficient in scope that they are consistent with the requirements of Atos CDC. Specifically, all parties making direct use of the e-Bulk service (Registered Bodies and Umbrella Bodies connecting their systems to the e-Bulk interface, including DBS), and therefore communicating via the CDC MFTS, must comply with the relevant requirements of the CDC Code of Connection.

DBS, as the only signatory, will need to fully comply to the CDC Code of Connection [6]

The specific requirements of the CDC Code of Connection to which all other parties using the e-Bulk service must comply are:

i) If an e-RB modifies the connection, software or hardware of their system connected to e-Bulk or makes any changes to connections to the e-Bulk server they must report a service incident and inform DBS First Line Support according to the procedure defined in 7.6.

ii) Atos will perform an IT Health check on each instance of CDC, where issues are raised that are caused by customer code, then as a minimum issues that are classified as high must be resolved before e-RB go live and remediation plans must be in place to resolve all medium issues.

iii) All parties using CDC are required to follow the published guideline for deployment into CDC [7].

iv) RB applications that are to be connected to CDC must meet the following conditions:

- RB application must not require to run with 'root' or 'admin' privileges;
- The RB application must operate through the Atos Secure Cloud (ASC) boundary protection.

## 2.3 Data Protection Act 1998

E-RBs have responsibilities under the Data Protection Act 1998 in accordance with the information classification noted above. It is each e-RB's responsibility to ensure that they comply with the requirements of the Data Protection Act 1998 in respect of data collected for, received from and exchanged over the e-Bulk interface.

The DBS is fully committed to compliance with the Data Protection Act 1998. Appropriate measures are in place to ensure that data is both processed and stored in accordance with this Act.

## 2.4 Notice to Applicants

The e-Bulk service can in nearly all circumstances eradicate the need for a DBS application form, each e-RB, when obtaining information that will be used for a DBS Check, must ensure that they make available, to each applicant, the DBS statement of fair processing relating to their application. E-RBs should outline what and how information is going to be processed. This is to make sure the individual knows exactly what is going to happen to their information and how it is going to be used. E-RBs should not be doing anything with personal information unless the individual is made aware (unless certain exemptions apply). The statement of fair processing is provided at Annex A. The statement of fair processing should be made available during the Business Assurance Gateway process.

The DBS will not uphold Data Entry disputes[1] where the application was made via e-Bulk, unless the information has been subsequently amended incorrectly by DBS. Where complaints occur due to information being incorrect, the e-RB must be able to demonstrate that the information submitted using the e-Bulk system differs from what appears in the e-Result or the applicant's DBS Certificate. Where disputes are upheld by DBS another e-result will be issued.

## 2.5 Code of Practice

Registered Bodies processing e-Bulk applications under this Agreement must ensure that they continue to adhere to the DBS Code of Practice and Guidance as an integral part of the conditions of their registration with the DBS. The Code and Guidance address the specific requirements incumbent on Registered Bodies in respect of:

- Identity Verification
- The management and use of disclosed information
- The Eligibility of positions or employment

[1] Data entry disputes are those where the applicant or RB challenge that the data which appears on the DBS Certificate or e-result was not the data they submitted for the application.

- The Payment of Fees
- Assessing the Suitability of individuals for such positions or employment
- The assessment of the suitability of RBs for ongoing registration with the DBS via the assurance and compliance process

## 2.6 Countersignatory Responsibilities

Countersignatories have responsibilities, as laid out in the Code of Practice and accompanying guidance.

Applications submitted via e-Bulk are electronic and, therefore, have no written Countersignatory signature. However, the Countersignatory number must be provided in the correct place within each e-Bulk application to indicate which Countersignatory has validated the application [2]. Provision of the Countersignatory number in this way conveys acceptance, by the respective Countersignatory, of their responsibilities as a Countersignatory of the application and equates to the declaration on the existing paper DBS Application Form. For this reason, the DBS requires that e-RBs account for this in their procedures and e-Bulk solution, ensuring that each Countersignatory conducts the actions, supported by the e-RB IT system, to apply their particular Countersignatory number and that safeguards are in place to ensure that only they can apply their Countersignatory number to applications, prior to their submission over the e-Bulk interface.

If an individual Countersignatory is suspended from submitting Disclosure applications the same will apply to their e-Bulk status. Any e-Bulk applications made by a suspended Countersignatory will automatically fail business validation rules and the e-applications will not be accepted.

## 2.7 Termination of Service

The DBS reserve the right to temporarily or permanently disable an e-RB from using the e-Bulk service and request that all applications are submitted on a paper DBS application as and when deemed appropriate by the DBS. The e-RB will be notified of the decision and if appropriate, reasons why. This applies to individual e-RBs and the e-Bulk service in its entirety. For individual cases a right of appeal against the decision to disable an e-RB will be available through the First Line Support helpdesk.

## 2.8 Electronic Evidence of Applicant Declaration & Consent

Should the DBS need to pursue a prosecution for identity crime, it will require proof that an applicant has provided a signed declaration and consent on a particular date. This has previously been evidenced via the Application Form and dated signature. However, under e-Bulk this information will no longer be presented to DBS.

Therefore, in all circumstances, it will be necessary for e-RBs to provide evidence to DBS on request for prosecution and possibly for use in a court of law. Where paper application forms and written signatures continue to be used, there will be a requirement for these to be presented to the DBS on request for this purpose. Where an electronic system has replaced the use of paper forms and written signatures, e-RBs will be required to provide evidence of the signed declaration and consent and this must be kept for 12 months. This will state that on a given date, the applicant:

- Represented his/her identity to be true,
- Gave a declaration about the information he/she provided,
- Gave consent for the application,
- Corroborated his/her identity to be true via documentation.

Electronic systems must therefore provide an electronic equivalent to a signature. This may be via a tick box to demonstrate that the applicant gave their declaration and consent on a particular date and time. If a tick box is used, then it must default to ‘not ticked’ and require a positive action on the part of the applicant to tick it. For this to be valid, the system would have first authenticated the applicant e.g. by use of user name and password. The RB must be able to demonstrate that the applicant had been informed not to disclose these details. In the case that the applicant requires and has declared a representative (e,g, due to language difficulties or disability) then a full audit trail of consent must be made available if requested by DBS. As, in some cases of disability, it will not always be possible to obtain written confirmation of consent from an applicant who requires assistance in the completion of their application, it is permissible in these circumstances for verbal consent only to be obtained – relevant audit trail should however contain confirmation of the identity of the individual who obtained and recorded this consent and this should be retained for 12 months from the date on which the consent was obtained. The e-RB must also provide an electronic signature to confirm that they have performed an identity check, which must also be date and time stamped

Whether using paper or electronic systems, these details must be retained for a period of 12 months.

# 3 Volumes & Frequency

Once a new e-RB is connected to the live e-Bulk service, a probationary period will apply within which time the DBS will routinely assess the quality and accuracy of each submitted application. During this period the number of e-bulk applications that the RB may submit will be capped by the DBS. Notification of the initial duration of the probationary period and the maximum number of applications that can be submitted within that period will be forwarded to e-RBs at the conclusion of the Business Assurance Gateway process. Once an e-RB has been successful in meeting the required quality and accuracy standards within a probationary period, the DBS will forward confirmation removing the limit on the maximum number of applications which can be forwarded via the live e-Bulk service.

One of the criteria that determines eligibility to be an e-RB is volume of DBS applications. E-bulk is available to RBs who have submitted in excess of 1500 applications in any rolling 12 month period in the last 18 months. It is expected that e-RBs will submit the vast majority of their applications using e-Bulk. DBS will continue to monitor e-RBs usage of the service and if necessary work with e-RBs to increase their percentage usage of e-bulk applications.

e-RBs are expected to aggregate e-Bulk applications into batches (up to a maximum permitted batch size, as described in [2]). The applications are then submitted, in these batches, over the e-Bulk interface. If a batch reaches the maximum size it should be submitted to DBS and subsequent applications aggregated into a further batch (and this repeats each time a batch becomes full).

To avoid unnecessary network traffic, e-RBs are expected, in normal circumstances, to send partially filled batches (those that have not reached the maximum batch size limit) no more than once per day. Batches that have reached the maximum batch size limit must be submitted on the same day. e-RBs must avoid the stock piling of batches.

This does not preclude the sending of batches containing as little as a single application outside of the daily submission frequency, in exceptional circumstances, in order to prioritise specific applications.

RBs should be able to configure the maximum number of applications per batch.

The DBS will batch messages sent to e-RBs in a similar manner on a per RB basis. The principle is, therefore, the same, i.e. that e-RBs will (unless there are no messages to send on a particular day) receive messages in the form of a daily batch, but will receive more than one batch if maximum batch sizes are exceeded.

E-RBs must make a connection to the DBS MFTS to determine if there are messages for them to retrieve and must then pull any messages that are waiting. Although the intended approach for e-Bulk is a daily exchange of data (and the DBS recommends that e-RBs retrieve waiting messages no less often than once per working day), the DBS recognises that some RBs, particularly those submitting higher volumes of applications and therefore more likely to receive multiple batches of a given message type per day, may wish to 'poll' for messages more frequently than daily.

The DBS may request e-RBs use certain time periods each day to submit applications and poll the exchange. This is to allow capacity management of the end to end service once a large number of e-RBs are using the service.

The service will not be available during the Atos standard maintenance windows; which are Thursdays 1800-2100 hrs. Atos may also need to schedule maintenance windows at weekends, but this will be by arrangement.

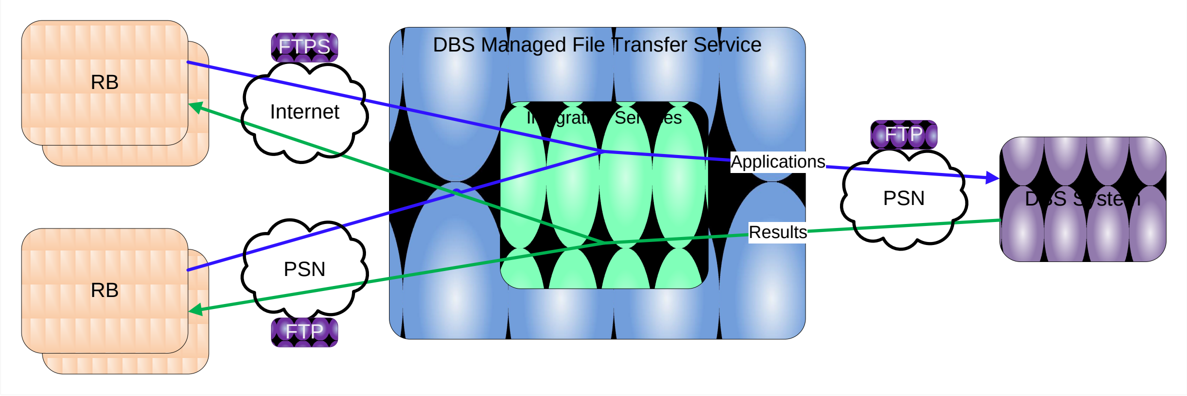
# 4 Message Delivery Mechanism

This section describes the mechanisms, such as message transport and network connectivity, that support delivery of messages between e-RBs and the DBS's e-Bulk service.

## 4.1 Use of DBS Managed File Transfer Service (MFTS)

The B2B (Business to Business) channel that is provided for use, by e-RBs, of the e-Bulk service will be routed through the CDC MFTS and exploit facilities and protocols provided by that service.

The following diagram illustrates the position of the DBS MFTS in the e-Bulk service.



## 4.2 Network Connectivity

Data will be transferred between e-RBs and the DBS MFTS either through the Public Services Network (PSN), for those RBs that have an approved connection to PSN, or over the Internet using the secure Internet transfer facilities provided by the DBS MFTS. Both mechanisms provide a secure connection between each e-RB and the DBS MFTS.

Data will be transferred between the DBS and the DBS MFTS through PSN, providing a secure connection for this communication.

## 4.3 Transport Mechanism

The protocol used for transporting messages between e-RBs and the DBS MFTS, where the RB is connected via PSN, is FTP. The message transport mechanism for e-RBs connected over PSN is defined in detail in **Error! Reference source not found.** and [5] and e-RBs connected over PSN must conform to the protocols described in these documents.

The protocol used for transporting messages between e-RBs and the DBS MFTS, where the RB is connected via the Internet, is FTPS. The message transport mechanism for e-RBs connected over the Internet is defined in detail in [4] and [5] and e-RBs connected over the Internet must conform to the protocols described in these documents.

# 5 Message Processing

This section describes the processes, rules and responsibilities that govern the processing of the business messages exchanged between end-points of the e-Bulk interface.

## 5.1 Message Exchange Business Process

The exchange of messages over the e-Bulk interface will follow the business process flows defined and described in [1].

## 5.2 Message Format

The messages exchanged over the e-Bulk interface will adhere to the XML formats defined and described in [2].

## 5.3 Message Validation

### 5.3.1 Messages from e-RB to DBS

The DBS will validate eBulkApplicationsBatch messages received from e-RBs at message (file- / batch-) level and also, where that has succeeded, at individual application level, as described in [1] and [2]. This includes validation that messages are compliant with the format and, in particular, XML schema definition described in [2], validation of filename format and, at application-level, additional business validation.

Where message-level validation fails, the DBS will respond with an EBulkApplicationBatchRejection message that will provide the reason(s) that the message failed this validation.

Where application-level validation fails for a particular application, the application receipt returned for that application will indicate rejection of that application and provide the reason(s) that the application failed this validation.

In the event of message or application rejection, e-RBs should rectify the problem(s), seeking support from their local helpdesk / service desk. When such local channels of support have been exhausted and assistance is required from DBS the e-RB should follow the procedures set out in section 7.6. In the case of rejection of an individual application (as a result of application-level validation), the corrected application may be re-submitted with its original RB application reference.

e-RBs are required to apply XML schema and business validation to each message that is to be sent from the e-RB to the DBS. Messages must pass this validation before they are sent over the e-Bulk interface. If a message fails this validation, the problem must be investigated by the e-RB from their local helpdesk / service desk. When such local channels of support have been exhausted and assistance is required from DBS the e-RB should follow the procedures set out in section 7.6 and rectify the incident before the message is re-sent.

The DBS may contact an e-RB to investigate the matter if messages from the e-RB are failing validation when received at the DBS.

### 5.3.2 Messages from DBS to e-RB

The DBS will apply XML schema validation (as per the format and XML schema definitions defined in [2]) to each message that is to be sent over e-Bulk to an e-RB. Any messages that fail this validation will not be sent and the DBS will take steps to rectify the problem.

e-RBs must apply XML schema validation (as per the format and XML schema definitions defined in [2]) to each message received from the DBS. Any messages that fail this validation should not be processed and the issue should be raised as a service incident according to section 7.6. Where the issue affects more than one e-RB the DBS will communicate the issue and proposed resolution time to all e-RBs.

## 5.4 Message Integrity

The DBS will verify the integrity of e-Bulk messages received from e-RBs, as described in [3] and will:

- Permit processing to continue for messages that are successfully verified.
- Investigate any occurrences where integrity verification fails.

The DBS will also add integrity protection to e-Bulk messages that it sends to e-RBs [3].

e-RBs must verify the integrity of e-Bulk messages received from the DBS [3]:

- In any and all cases where this check fails, the e-RB must raise the issue as soon as possible as a security incident, according to section 7.6
- If, and only if, this check succeeds, the e-RB can and should continue to process the message.

e-RBs must also add integrity protection to e-Bulk messages that they send to the DBS [3].

## 5.5 Additional Guidance on data to be collected by e-RBs

This section provides additional guidance on the data that e-RBs may collect from applicants for the DBS application.

Note that the DBS application includes data fields that are mandatory if applicable. These items are not enforced as mandatory in the e-Bulk Application message XML schema definitions, as there are legitimate circumstances in which a value may not be provided for them, but a value must be provided if applicable to the applicant.

### 5.5.1 Passport Details

Passport details are optional within the message format for submission of applications over e-Bulk, as defined in [2]. However, the DBS requires that e-RBs ask applicants whether they have a passport and capture passport details for those who indicate that they do have one. British or overseas passport details can be input but note that the data field is limited to 11 alpha numeric characters (including certain special characters i.e. hyphen). Only the first 11 characters should be input.

### 5.5.2 Driving Licence Details

Driving licence details are optional within the message format for submission of applications over e-Bulk, as defined in [2]. However, the DBS requires that e-RBs ask applicants whether they have a valid UK driving licence and capture the details for those who indicate that they do. In these cases, the driving licence number provided must be validated by the e-RB processes. This is carried out by additional business validation that must be applied by e-RBs according to the UK driving licence formatting rules that are defined in [2][1].

If this driving licence validation is not passed, the application must not be submitted and the e-RB must re-check the applicant's identity details to determine why there is a mismatch. If there is a legitimate reason for the discrepancy, the application must not be submitted using e-Bulk (a paper application should be used). Otherwise, the details in the application should be corrected and re-validated before submitting the application using e-Bulk.

An E-RB may accept a non-UK Driving Licence for information purposes but this cannot be used for identification purposes.

### 5.5.3 Singular Names

If it is the intention of the e-RB to allow applicants who only have one single name to submit applications using the e-Bulk interface the e-RB must provide guidance to applicants confirming the one name should be input into both the surname and forename fields in order to ensure the file meets the validation rules. Applicants must be advised that having submitted the application in this way the e-Bulk Result will also have the same name populated in both the forename and surname field.

[1] Note that this is dependent on the update to the BMS being approved.

# 6 Service Management

This section is concerned with the Service Management processes related to the operational running and maintenance of the e-Bulk service. It contains headings for each recognised service area and, within each subsection, considers the related roles and responsibilities of the parties to this Interchange Agreement.

## 6.1 Service Level Scope

Each e-RB must have a local service desk that must act as first line support for the e-RB organisation. This local service desk will be the e-RB's point of contact with the DBS first line support helpdesk service provided to e-RBs. Each e-RB is required to nominate two individuals who have authorisation to report to the DBS first line support helpdesk all security incidents, service incidents and service requests as defined in 7.6. These should be the same individuals who have access to the secure email account provided through the DBS.

An executive within the RB who has responsibility and accountability for security must also be nominated.

## 6.2 Incident Management

Incident Management is the process of managing unexpected operational events, with the primary objective of returning service to users as quickly as possible.

An *incident* is defined as: "any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service".

Each e-RB will be responsible for operating Incident Management in terms of the e-RB's own infrastructure, including that which underpins its use of the e-Bulk interface, as agreed between the e-RB and their in-house IT support capability and/or third-party supplier(s).

The DBS will be responsible for operating Incident Management in terms of the provision of the e-Bulk interface itself, as agreed between the DBS and its partners and suppliers.

If an incident with the e-Bulk service is identified, the party identifying the incident must first investigate whether the fault lies on their side of the service boundary:

- In the case of an incident being identified by an e-RB, this means that initial investigation is undertaken by the e-RB and their first line support provider.
- In the case of an incident being identified by the DBS or its partners /suppliers, this means that initial investigation is undertaken according to the incident management procedures agreed between the DBS and its partners /suppliers.

Where it is not possible for one side of the service boundary to determine where the source of the incident lies or where it is identified that the incident lies across the service boundary, the incident will be escalated between the parties in accordance with section 7.6

## 6.3 Problem Management

Problem Management is the process that identifies the root cause of one or more existing or potential incidents. Problems may be identified as a result of multiple incidents that exhibit common symptoms or identified from a single significant incident, indicative of a single error, for which the cause is, as yet, unknown. Problems may also be identified before any related incidents actually occur.

Each e-RB will be responsible for operating Problem Management in terms of the e-RB's own infrastructure, including that which underpins its use of the e-Bulk interface, as agreed between the e-RB and their in-house IT support capability and/or third-party supplier(s).

The DBS will be responsible for operating Problem Management in terms of the provision of the e-Bulk interface itself, as agreed between the DBS and its partners / suppliers.

If a problem with the e-Bulk service is identified, the party identifying the problem must first investigate whether the fault lies on their side of the service boundary:

- In the case of a problem being identified by an e-RB, this means that initial investigation is undertaken by the e-RB and their first line support provider.
- In the case of a problem being identified by the DBS or its partners /suppliers, this means that initial investigation is undertaken according to the problem management procedures agreed between the DBS and its partners/suppliers.

Where it is not possible for one side of the service boundary to determine where the source of the problem lies or where it is identified that the problem lies across the service boundary, the problem will be escalated between the parties in accordance with section 7.6.

## 6.4 Change Management

Change Management is the Service Management process responsible for controlling and managing requests to make changes to the IT infrastructure or, indeed, any aspect of the IT services that are in scope in order to bring about business benefit whilst minimising the risk of disruption to services. Change Management also manages the implementation of such changes that are given the associated approval.

Each e-RB will be responsible for operating change management in terms of the e-RB's own infrastructure, including that which underpins its use of the e-Bulk interface, as agreed between the e-RB and their in-house IT support capability and/or third-party supplier(s).

The DBS will operate a change management process in respect of the e-Bulk service and its provision, in conjunction with its partners/suppliers. This change management process will consider the handling of each potential change based upon an assessment of that change. Impact assessment of each change will determine whether the change should proceed, whether further assessment through consultation with other parties, including e-RBs, is required and whether there are interested parties for whom only notification of the planned change is required. This assessment will also determine the notice period to be given.

The DBS will be responsible for communicating planned changes to those impacted (or potentially impacted) and consulting with others to further assess the change where this is required. How these matters will be communicated to e-RBs is described in section 7.6.

The scope of this change management process includes changes to e-Bulk specifications and other e-Bulk documentation, including this Interchange Agreement.

### 6.4.1 Change Originating from DBS (or DBS's partners / suppliers)

Changes to e-Bulk originating within the DBS or initiated by its partners / suppliers will be subject to the DBS change management process for e-Bulk. All changes will be assessed based on priority, benefit, complexity and impact (including their impact on e-RBs, the DBS and its partners / suppliers). DBS will inform e-RBs of changes by other parties (e.g. DBS partners / suppliers) that could affect them. The e-RB should assess these changes and respond within 5 working days if there may be an adverse impact, otherwise the change will be deemed accepted by the e-RB.

### 6.4.2 Change Originating From e-RBs

This section is concerned with changes originating from an e-RB that have an impact on the configuration of the e-Bulk service. In general, the impact of these changes will be constrained to the configuration of the e-Bulk service for the originating e-RB and to the same e-RB's own system. These would include small configuration changes (e.g. change of IP address) and more significant changes (e.g. significant e-RB system changes such as the addition of a web portal) which would require some re-testing with e-Bulk. In such situations the DBS reserve the right to charge to the e-RB any associated costs which may be incurred by the DBS.

The DBS must be informed of these changes 28 days prior to the planned change according to the procedures defined in 7.6.

DBS will impact assess any such changes and where necessary may ask the RB to complete and / or re-sign certain documentation e.g. complete a new Business Assurance Gateway questionnaire.

Note that RBs, including e-RBs, have existing responsibilities under the Code of Practice in respect of changes to their status as RBs, including responsibilities to notify the DBS of changes to countersignatories, organisation name and so on. The procedures associated with these are not altered by e-Bulk, and the definition of these responsibilities and processes is outside the scope of this document.

Likewise, this section is not concerned with suggestions for changes to improve the e-Bulk service (see following section 6.4.3).

### 6.4.3 RB Suggestions

The DBS continually seeks ways to improve services that it offers and will consider suggestions raised by e-RBs concerning the e-Bulk service. These can be raised via the first line support helpdesk provided to e-RBs, as described in 7.6. Note, however, that the raising and initial consideration of these suggestions fall outside the scope of the normal change management process.

## 6.5 Configuration Management

Configuration Management is the process of planning for, identifying, controlling and verifying the configuration items within a service, recording and reporting their status and, in support of change management, assessing the potential IT impact of changing those items.

Each e-RB will be responsible for Configuration Management of its own infrastructure that underpins its use of the e-Bulk interface, as agreed between the e-RB and their in-house IT capability and/or third-party supplier(s).

The DBS will be responsible for Configuration Management in terms of the provision of the e-Bulk interface itself, as agreed between the DBS and its partners/ suppliers.

## 6.6 Release Management

Release Management covers the planning, design, build, configuration and testing of hardware and software releases to create a defined set of release components.

Each e-RB will be responsible for Release Management for its own infrastructure that underpins its use of the e-Bulk interface, as agreed between the e-RB and their in-house IT capability and/or third-party supplier(s). As well as the Technical Assurance Gate (TAG) required before an e-RB can go live or following a significant system change as in 6.4.2, DBS will also carry out a Business Assurance Gate (BAG) to ensure that business processes have been implemented to address:

- data quality and verification;
- applicant’s consent and declaration;
- ability to present an audit trail from the declaration to the electronic submission which can be kept for a maximum of 12 months;
- the requirement for each e-RB to have a written security policy;
- an individual has been nominated for key management and an appropriate audit trail is available which can be kept for a maximum of 6 months;
- a key management process is in place.

Where e-RBs suspect that a software or hardware change may require re-testing, they must inform the DBS so that an assessment can be made on effort and costs involved.

The DBS will be responsible for Release Management in terms of the provision of the e-Bulk interface itself, as agreed between the DBS and its partners and suppliers.

Note that the impact on other parties of implementing releases will be dealt with by Change Management (see section 6.4)

## 6.7 Service Level Management

Service Level Management is the process of defining, agreeing, documenting and managing levels of customer service that are required and cost justified.

Each e-RB will be responsible for Service Level Management for its own infrastructure that underpins its use of the e-Bulk interface, as agreed between the e-RB and their in-house IT capability and/or third-party supplier(s).

The DBS will be responsible for Service Level Management in terms of the provision of the e-Bulk interface itself, as agreed between the DBS and its partners / suppliers.

The DBS will manage target service levels for the first line support helpdesk provided to e-RBs.

## 6.8 Service Reporting

Service Reporting is the process of documenting and reporting any aspects of Service Management.

Each e-RB will be responsible for Service Reporting for its own infrastructure that underpins its use of the e-Bulk interface, as agreed between the e-RB and their in-house IT capability and/or third-party supplier(s).

The DBS will be responsible for Service Reporting in terms of the provision of the e-Bulk interface itself, including the first line support provision, as agreed between the DBS and its partners and suppliers.

## 6.9 Capacity Management

Capacity Management is the process for defining the business's requirement for IT capacity, in both business and technical terms.

Each e-RB will be responsible for Capacity Management for its own infrastructure that underpins its use of the e-Bulk interface, as agreed between the e-RB and their in-house IT capability and/or third-party supplier(s).

The DBS will be responsible for Capacity Management in terms of the e-Bulk interface itself, as agreed between the DBS and its partners /suppliers. The DBS will continue to work with e-RBs to forecast and plan for ongoing volumes of DBS applications.

## 6.10 Security Management

Security Management is the process of ensuring that services are used in an acceptable manner, are compliant with applicable legislation, and are used and accessed only by those people permitted to do so, to ensure appropriate protection of the confidentiality, integrity and availability of information assets and associated infrastructure.

Each e-RB must operate local security management procedures in accordance with their security policy.

The DBS will operate security management procedures in accordance with its own security policy and according to agreements with partners / suppliers.

Security incidents occurring within the e-RB's infrastructure connected to the e-Bulk service must be reported according to the security incident reporting procedure defined in section 7.6. This especially applies in the case of actual or suspected virus / malware infection and actual or potential compromise.

## 6.11 3rd Party Data Processors / Suppliers

3rd Party Supplier Management is the process by which the DBS and the RB manage 3rd party suppliers. This is particularly in relation to the management and security of the delivery of DBS electronic application data.

If an RB's 3rd party data processor / supplier will have access to DBS electronic application data whether on an ad hoc or continual basis once that RB goes live, then the 3rd party data processor / supplier must be approved by the DBS before it is allowed to access DBS data.

The 3rd party data processor / supplier will be required to complete a pre-qualification questionnaire (PQQ) to enable DBS to assess its suitability to access DBS electronic application data. If approved, the 3rd party data processor / supplier will be asked to sign a contract with the DBS that sets out its obligations when accessing DBS data.

If the 3rd party data processor / supplier PQQ is not approved by the DBS the e-RB will be unable to use the e-bulk service until such a time that either:

i. the 3rd party data processor / supplier has taken the required actions to remedy the previous PQQ failure(s), has re-submitted an amended PQQ which has been approved by the DBS and has signed the requisite contract with the DBS;
ii. the DBS is satisfied that the e-RB has adapted its e-bulk system so there is no 3rd party supplier / data processor access to DBS electronic application data; or
iii. the e-RB has acquired the services of an alternative 3rd party data processor / supplier which has successfully completed the approval process.

If an e-RB using the live e-Bulk service subsequently decides to change their processes / system which would enable a 3rd party data processor / supplier to have access to DBS electronic application data the e-RB must inform DBS immediately, as the 3rd party data processor / supplier must follow the PQQ process and be approved by the DBS before access can be granted.

All RBs/e-RBs must consider carefully before committing to use a 3rd party data processor / supplier it's appropriateness and likelihood of successfully completing the DBS's approval process. Copies of the PQQ, contract and supporting guidance are available on the DBS website. RBs/e-RBs are strongly advised to provide a copy of these documents to any prospective 3rd party suppliers in advance of making any commitment. The DBS accepts no liability whatsoever to the e-RB in the event that a 3rd party data processor / supplier fails the approval process.

Should an e-RB plan to make any changes to their e-bulk system / processes at any time in the future which would involve the introduction or removal of a 3rd party having access to DBS electronic application data, they must seek further guidance available on the DBS website.

To ensure that RB's/e-RBs do not procure the services of a 3rd Party supplier without DBS knowledge, DBS have instructed the Atos not to connect any 3rd Parties which have not been approved by DBS. This is essential in maintaining the security and integrity of the e-Bulk service.

# 7 Supporting Procedures

In general, supporting procedures relating to applications submitted electronically over e-Bulk will be the same as those that apply for applications submitted using the established paper-based DBS application process. This section summarises key additional procedures that apply to e-Bulk. The detail of these procedures is covered in documentation that is referenced below.

## 7.1 Administrative Errors & Corrective Actions

In the event that applications submitted electronically over e-Bulk are submitted in error but have been accepted for processing (e.g. a keying error is identified by the e-RB *after* submitting an application), any process that applies in order to correct this situation will be as for the paper DBS application process (this includes any impact on fees). It is, therefore, important that applications are adequately checked and validated before submission.

DBS intend to monitor closely all e-Bulk applications during the first few weeks following an e-RB going live or following a major system release. Error rates should not increase above the e-RB’s current error rate for paper applications following e-Bulk implementation or exceed 1% of the total number of applications submitted. Where e-RBs breach this level, access to the e-Bulk service may be disabled whilst any problems are remedied. In serious cases this could lead to permanent withdrawal of the service. This will be assessed on a per e-RB basis. Please refer to section 2.7.

## 7.2 Exception Handling & Validation Procedure

Use of the e-Bulk service must follow the process flows described in [1]. Upon receipt at the DBS, batches of applications will be validated. This validation will have multiple stages and will allow for rejection of entire batches or individual applications within a batch. The outcome of this validation will be reported over the interface according to the process described in [1].

Messages exchanged over e-Bulk must conform to the relevant message format defined and described in [2], and e-RBs must apply XML schema validation to messages, before submitting them over the interface, thus ensuring that they are conformant with the relevant message format.

e-RBs must also apply additional business validation, as defined in [2], to applications before they are submitted over e-Bulk. One of the major benefits of this electronic application route is that these kinds of validation can be automated in order to minimise the number of applications containing errors that are submitted.

## 7.3 Error Correction

If submission over e-Bulk of a batch of Disclosure applications yields errors that result either in rejection of the entire batch or in rejection of individual applications (with notification of these rejections being returned over the interface), the e-RB may, if able, correct the problem(s) that caused the rejection and re-submit those applications that have not been accepted for processing. In the case of rejection of an entire batch, the entire batch or a subset thereof may be re-submitted.

In the event that the e-RB is unable to correct the problem or in the event of any other error detected either by the e-RB or the DBS, the error will be raised as a support incident following the processes defined in section 7.6.

## 7.4 Fallback Procedure

E-RBs must consider and have in place a Business Continuity Plan. If an e-RB finds it necessary to instigate their business continuity plan, DBS must be informed as soon as possible using the incident reporting procedure described in 7.6.

If the e-Bulk service is rendered unavailable by the DBS for a period of more than 5 working days, the fallback will be to submit applications using the established paper application process, which will remain in operation alongside the e-Bulk service. In the event that this fallback is used, e-RBs are permitted to send by post either a handwritten or overprinted DBS Application Form which must be signed by the applicant and Counter Signatory. The resulting DBS certificate will also be issued by means of the established paper process.

Notification to e-RBs of service problems leading to extended unavailability will be carried out as described in 7.6.

In the event that an e-RB incurs a double-charge for an application as a necessary consequence of extended e-Bulk unavailability caused by DBS or its partners / suppliers (e.g. an application submitted via e-Bulk has to be re-submitted by paper form), the e-RB may request a credit using the normal process for DBS invoice queries.

E-RBs must keep copies of all XML files sent to the DBS together with logs of what was sent and when, in case the applications have to be re-sent. Ideally these should be kept until the application has been through the entire process and in line with the Code of Practice in general this should be no longer than 6 months.

E-RBs should consider contingency planning when introducing hardware/ software changes so if necessary they can revert to previous systems in order for their e-bulk service to be maintained.

## 7.5 De-registration from e-Bulk

In the event that an e-RB no longer wishes to use the e-Bulk service and wishes to be disabled from the e-Bulk service, the Lead Signatory should contact the DBS according to the published procedure (described in 7.6.3) requesting to be disabled from e-Bulk.

Note that if an e-RB ceases to be an RB (or UB), their eligibility to use the e-Bulk service also ceases.

## 7.6 Incident Reporting Overview

The e-RB must report security and service incidents as described throughout this document. The e-RB may continue to use their Criminal Justice Secure eMail (CJSM) email account for the sending / receiving of information up to and including “Restricted” or “Official - Sensitive” (Details relating to the current Government security classifications can be found at https://www.gov.uk/government/publications/government-security-classifications) once they have gone live on the e-Bulk interface. The e-RB will report any compromise or potential compromise to the e-Bulk service as soon as it is identified. In the first instance this should be done by telephone. E-RBs are not permitted to document sensitive information including personal data via non secure e-mail or facsimile. Incidents which occur without warning should be communicated to the first line support helpdesk via telephone. If the e-RB is aware of an incident in advance this must be brought to the attention of the first line support team immediately in writing via CJSM secure email. The e-RB should report the nature of the incident, when it was first discovered, how it happened and how many applications could be potentially impacted including details of the unique reference number(s) and any other details of the application(s). The DBS first line support team will work with the e-RB to resolve the issue. The e-RB should make every effort to provide adequate resource to assist in resolving the issue. Failure to do so may result in the e-RB being disabled from using the e-Bulk service. Please refer to section 2.7.

The DBS will report incidents and communicate planned changes to e-RBs either directly to the e-RB via telephone or email where appropriate; e-Bulk documents published on GOV.UK will be updated when required. Incidents will be assessed and where possible a period of notice will be given prior to changes being implemented. Where necessary the DBS reserves the right to revert to the fallback procedure as defined above in section 7.4. It is the responsibility of the e-RB to check the published documents on GOV.UK for updates.

### 7.6.1 Reporting Availability

The DBS first line support helpdesk function will be available Monday to Thursday 9am – 5pm and Friday 9am – 4:30pm and will be contactable via telephone, facsimile and secure e-mail with the provision that sensitive information must not be disclosed via a non secure email address, telephone or facsimile. Service requests and service incidents should be reported within these times or the next available working day. Contact details for the first line support team will be provided to each e-RB the day they are enabled on the live e-Bulk service.

### 7.6.2 Reporting Security Incidents

A security incident is any incident that threatens computer assets, networks, information systems and data integrity such as message integrity failure, key compromise, key revocation, intrusion detection system alerts and virus infection. The e-RB has a duty in the case of a security incident or potential security incident to raise a call with the DBS first line support helpdesk as soon as the incident is identified. This can be done via telephone, facsimile, letter and secure e-mail with the provision that sensitive information must only be disclosed via secure email.

Where an e-RB requires a new integrity key to be issued they should contact DBS stating why a new integrity key is required and the date the integrity key is to be effective from.

All requests for integrity keys which are due to expire should be made to the first line support helpdesk at least 10 working days in advance of the expiry date. The e-RB will be notified when the key has been sent and should notify the first line support helpdesk if the key has not been received within 5 working days. In all cases the e-RB has a responsibility to contact the DBS and confirm receipt of the integrity key.

If an e-RB wishes to disable their e-Bulk status the Lead Signatory should contact the DBS in writing. The first line support helpdesk will provide guidance on how to return or destroy the integrity key

### 7.6.3 Reporting Service Incidents and Requests

Service incidents relate to the operational running and maintenance of the e-Bulk service. Service requests are requests for a new or altered service. All requests must be made in writing via e-mail to the DBS. Where no sensitive information or personal data is included this can be done via a non secure email address. This includes changes to the preferred method of receiving results of the DBS check, requests for information, problem reporting, queries, complaints and suggestions. Where the RB wishes to change their preferred method of receiving DBS check results the RB will be notified of the decision and the effective date if applicable.

# 8 Guidance from DBS Certificate

The electronic result does not include the guidance that is on a paper DBS certificate. It should be noted therefore that this guidance is also applicable to electronic results. The guidance will continue to be printed on the paper DBS certificates issued to applicants.

For guidance on electronic results see section 9.4.

# 9 Additional Terms & Conditions

This section describes additional terms and conditions applying to use of the e-Bulk service that are not covered within the other sections of this Interchange Agreement.

## 9.1 Re-prints

The circumstances in which a re-print of a certificate can be requested are the same as those that apply to non e-RBs and the fully paper-based DBS application process. This also applies in the case of any applications that an e-RB submits using the paper-based application process.

In the event that an e-RB believes that an eBulkResult message has been sent to them but not received by them (e.g. by inferring this from the Online Tracking service), the issue should be raised in accordance with section 7.6. In such cases, where an eBulkResult does not instruct the e-RB to await presentation from the applicant of the paper certificate (‘blank’ results), re-prints will not be issued where it can be determined that the e-RB has collected the relevant eBulkResult message. (Where investigations find that transmission of an electronic result has failed en route to the e-RB, the resolution of this will re-send the electronic message if necessary.)

## 9.2 RB Entitlement to use e-Bulk

RB entitlement to become and remain an e-RB is subject to meeting DBS-defined criteria.

In particular:

- Should an e-RB cease to be an RB/UB, they will also cease to be an e-RB.
- E-RBs must use payment-on-account. Should an e-RB cease to use payment-on-account, they will lose their entitlement to use e-Bulk.
- If an e-RB fails to comply with the requirements set out in this Interchange Agreement, the DBS reserves the right to withdraw that e-RBs entitlement to use the e-Bulk service.

## 9.3 Equality & Diversity

The DBS strongly recommends to e-RBs that, when determining how data will be collected from applicants, they give due consideration to equality & diversity matters (e.g. with respect to: disability, race, gender, age, sexual orientation, religion).

The DBS has a confidential checking process for Transgender applicants who do not wish to reveal details of their previous identity to the person who asked them to complete an application form for a DBS check. This transgender process is not available through the normal paper or e-bulk application process. RBs should make applicants aware of this process. Further information is contained on DBS’s website regarding this process.

## 9.4 E-Results

The RB will receive an e-result for each application submitted to the DBS. The applicant will continue to receive a paper certificate containing the results of the DBS check. The e-result will contain the following attributes:

- DBS Application Reference Number
- RB Application Reference Number
- Disclosure Type
- Disclosure Number
- Disclosure Issue Date
- Applicant Names
- Applicant Date of Birth
- Applicant Place of Birth
- Gender
- Applicant Full Address (inc post code)
- Please wait to view applicant certificate
  or
- Certificate contains no information

The Code of Practice states that RBs must ensure that no reproductions of the Certificate or its content are made, including photocopies or scanned images, unless with the prior agreement of the DBS or as a result of a stipulated requirement relating to the e-channel service.

E-RBs are therefore permitted to produce one copy of the e-Result in order to satisfy themselves or any other relevant party that a DBS check has been conducted, including for the purpose of complying with the requirements of regulatory inspection (e.g. by Care Quality Commission [CQC], Office for Standards in Education [OFSTED] or Care and Social Services Inspectorate in Wales (CSSIW). E-RBs must note that the rules concerning retention of DBS Certificate information as stated in the Code of Practice also apply to printed e-Results.

DBS issue e-Results to the e-RB in XML format and the mechanism by which an e-Result is produced in a readable format by the e-RB is outside the scope of the e-Bulk service.

### 9.4.1 Format of Notification

The electronic contents can be included in a letter or document with the proviso that the DBS logo should not be used. The DBS logo is a registered trademark in the United Kingdom. The DBS does not allow or permit Registered Bodies to use this logo. It should have a statement at the beginning of the document that says ‘This is not a Certificate issued by the DBS’. Neither the document nor associated guidance on the back of the DBS Certificate should be reproduced in such a way that an individual or organisation could believe it to be a DBS certificate within the meaning of sections 113A 113B 114 and 116 of the Police Act 1997.

### 9.4.2 E-result scenarios

An e-result can contain 2 types of messages. Scenario A - If there are no matters to record the e-result will contain the words ‘Certificate contains no information’.

Scenario B - If there are matters to record the e-result will contain the words ‘Please wait to view applicant certificate’.

### 9.4.3 Scenario A - Information That Can Be Included

Applicant Personal details: Forenames/Surnames
Date of Birth
Place of Birth
Gender
Address details
DBS result issue date
DBS certificate number
Level of check
No match exists for this person in the following fields:
Police National Computer
DBS Children Barred List
DBS Adults Barred List
Name of the Employer
Workforce
Position Applied For

If a barred list check was not requested then the wording “*not requested”* can be written alongside the appropriate list
e.g. DBS Children Barred List Not requested

### 9.4.4 Scenario B - Information That Can Be Included

You applied for a Certificate for the following individual:
Applicant Personal details: Forenames/Surnames
Date of Birth
Place of Birth
Gender
Address details
Level of check
Name of the Employer
Workforce
Position Applied For

DBS have notified us on dd/mm/yy that we must wait to view the applicant’s certificate.

9.4.5 An example of your notification must be made available as this will be requested as part of the BAG process.

# 10 Annex A

## Statement of Fair Processing

The Disclosure and Barring Service will refer the details provided on this application form to government and law enforcement bodies in accordance with any relevant legislation. The details provided to these bodies will be used for identifying possible matches to records held by them. Where such a match is established, data may be released to the DBS for inclusion on any certificate issued. The details provided on this form may be used to update the records held by the bodies specified above. The details provided on the application form may be used to verify your identity for authentication purposes. The DBS may use any information provided by the DBS on a certificate or otherwise held by the DBS to inform any of its barring decisions made under its powers within the Safeguarding Vulnerable Groups Act 2006.