Disclosure & Barring Service

Release 1 (R1) – Privacy Impact Assessment (PIA)

Version:	1.0
Date	22/12//2016

Synopsis:	Privacy Impact Assessment (PIA) conducted on Release 1 (R1) of the DBS Modernisation Programme
Document Status:	Final - Approved
Product Id:	DBS_STWR1_0293

Reviewers

No.	Name	Organisation/Role	Version	Issue Status
External Review				
01		Amnesty		
02		Liberty Human Rights		
03		Unlock		
04		Disclosure Scotland		
05		Access Northern Ireland		
06		Care Council Wales		
07		Education Workforce Council		
08		General Chiropractic Council		
09		General Dental Council		
10		General Medical Council		
11		General Optical Council		
12		General Osteopathic Council		
13		General Pharmaceutical Council		
14		General Teaching Council Northern Ireland		
15		Health and Care Professions Council		
16		Northern Ireland Social Care Council		
17		Nursing and Midwifery Council		
18		Pharmaceutical Society Northern Ireland		
19		NPCC		
20		Care and Social Services Inspectorate Wales		
21		Care Quality Commission		
22		Charity Commission		
23		Charity Commission for Northern Ireland		
24		Education and Training Inspectorate		
25		Estyn		
26		Health Inspectorate Wales		
27		National College for Teaching and Leadership		

28		Office of the Public Guardian		
29		OFSTED		
30		Regulation and Quality Improvement Authority		

Approvers

No.	Name	Organisation/Role	Version	Issue Status
01		DBS SIRO		Draft

Abbreviations

Acronym	Detail
DBS	Disclosure and Barring Service
HO	Home Office
PIA	Privacy Impact Assessment
ISA	Independent Safeguarding Authority
CRB	Criminal Records Bureau
IT	Information Technology
SVGA	Safeguarding Vulnerable Groups Act 2006
SVGO	Safeguarding Vulnerable Groups (Northern Ireland) Order 2007
R1	Release 1
TCS	Tata Consultancy Services
NCTL	National College for Teaching and Leadership
NAW	National Assembly for Wales
EWC	Education Workforce Council
SPS	Swiss Post Solutions
TI	Technical infrastructure
CRM	Customer Relationship Management
PLX	Police Local Exchange
TSQ	Telephone Security Questions
OBIEE	Oracle Business Intelligence Enterprise Edition
DPA	Data Protection Act
RAP	Regular Activity Provider
ANI	Access Northern Ireland
GTCNI	General Teaching Council for Northern Ireland

Contents

1. INTRODUCTION

1.1. The Disclosure and Barring Service (DBS)

The Disclosure and Barring Service (DBS) is a Non-Departmental Public Body (NDPB) and helps employers make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups, including children.

We are responsible for:

- Processing requests for criminal records checks (DBS checks)
- Deciding whether it is appropriate for a person to be placed on or removed from a barred list
- Placing or removing people from the DBS Children's Barred List and Adults' Barred list for England, Wales and Northern Ireland.

The Disclosure function of the DBS provides information to help employers make informed recruitment and licensing decisions, especially for those posts that involve working with vulnerable groups, including children. The Barring function of the DBS determines whether an individual can work in relevant posts by making suitability decisions about inclusion in one or both of the DBS Barred Lists.

The DBS undertakes legislative functions included within Part V of the Police Act 1997, the Safeguarding Vulnerable Groups Act (SVGA) 2006 and the Safeguarding Vulnerable Groups (Northern Ireland) Order (SVGO) 2007.

The Disclosure function searches police records, Disclosure Scotland records and in relevant cases, information held by the DBS Barring function, and issues a DBS certificate to the applicant.

The Barring function helps in the safeguarding of vulnerable groups, including children, from those people who work or volunteer with them and pose a risk of harm. The DBS may use any information on a disclosure certificate or otherwise held by the DBS to inform any barring decisions made under its powers within the SVGA and SVGO.

1.2. Release 1 (R1) Project

R1 is a technology enabled business change project that will deliver a new enhanced technology platform, re-engineered business processes and organisation change management. It will introduce new ways of working and will enable a modernised approach to the delivery of DBS services. Perhaps most notably for this document, it will introduce new methods of receiving, processing, storing and sharing data (including personal information) between DBS and various internal and external stakeholders and will transform DBS Barring from a paper based file system into a digital system. The expected date for transition is quarter four 2016.

1.2.1. IT Contractor

Tata Consultancy Services (TCS) is an Information Technology (IT) services, consulting and business solutions organisation that, in October 2012, was awarded the contract to manage the technology needs and some of the support services of the DBS.
Some of the additional responsibilities for TCS in R1 include the following:

- New dedicated technical infrastructure (TI) to include Production, Development, Test and Disaster Recovery (DR) environments.
- Ownership of current 'As-Is' TI hardware and software assets, in accordance with agreed commercial processes and procedures, in order to support the continued delivery of DBS services to be hosted at new data centres.
- Ownership of IT Service Management responsibilities for TI, local and business applications.
- Roll out of new customer contact centre telephony solution (STORM).
- Ownership of system and operational security responsibilities in accordance with DBS protocols and best practice.
- Ownership of management information solution (Data Warehouse) to ensure the continued delivery of operational MIS reporting.
- Upkeep of current external interfaces with Police National Computer Service (PNCs), Ministry of Justice (MOJ) and Local Police Forces (LPF) etc.
- Development of a new Disaster Recovery (DR) solution and Business Continuity Plan (BCP).
- Provision of new digital channels for DBS customers and individuals to contact DBS including a cloud based telephony solution, Web Chat, Short Message Service (SMS) and DBS Online Accounts (see section 4.1 for a description).

1.2.2. Other suppliers

Swiss Post Solutions (SPS) are a subcontractor of TCS and are responsible for the following:

- Document Management Solution (DMS) for the Disclosure service including Optical Character Recognition (OCR) scanning and printing.
- Application form, document and certificate printing and distribution.
- New scanning interface solution to provide clearer image resolution and legally admissible electronic records for all white mail.
- Scanning of existing barring case files
- New disaster recovery solution for scanning and printing.

DBS also use other suppliers as follows:

- British Telecom (BT) – Telephone lines
- Fujitsu – Desktops
- Vodafone – CJX connectivity
- Royal Mail – Incoming/outgoing post

- DPD – outgoing post
- TNT Business Solutions – Off-Site File Storage
- Home Office Technology (HOT)
- Hewlett Packard (HP)

1.3. Organisations DBS share information with

The DBS shares data with a number of partner and external organisations in order to deliver its legislative functions and in order to meet other organisations' legislative requirements placed on DBS.

The table below lists each organisation that the DBS either receives information from or provides information to. Further analysis of the risks and mitigation identified for each of these organisations can be found within Section 5.

Name	Acronym	Frequency
Referring Parties	RP	Ad hoc
Referred Individuals	RI	Ad hoc
Regulated Activity Providers	RAP	Ad hoc
Local Police Forces	LPF	Ad hoc
Police National Computer	PNC	Daily
Police Local Exchange	PLX	Daily
Police National Database	PND	Weekly
Home Office PNC Services	HOPNC	Ad hoc
Access Northern Ireland	ANI	Daily
Disclosure Scotland	DS	Daily
Keepers of Registers	KoR	Ad hoc
Supervisory Authorities	SA	Ad hoc
National College for Teaching & Leadership (formerly GTCE)	NCTL	Ad hoc
Education Workforce Council (formerly GTCW)	EWC	Weekly
General Teaching Council for Northern Ireland	GTCNI	Ad hoc
Tribunals - Barring Appeals (Upper Tribunal, Care Tribunal)	UT, CT	Ad hoc
National Assembly for Wales (Welsh Assembly)	WA	Ad hoc
Local Authorities	LA	Ad hoc
National Offenders Management Service	NOMS	Ad hoc
Probation Service	PS	Ad hoc
Department for Education	DfE	Ad hoc
Specialist Risk Assessors	SRA	Ad hoc
Prisoner Location Service	PLS	Ad hoc
General Register Office	GRO	Ad hoc
Independent Inquiry into Child Sexual Abuse	IICSA	Ad hoc
Registered Bodies	RB	Ad hoc
Disclosure Applicants	DA	Ad hoc
Amber Hill	AH	Ad hoc
Her Majesty's Passport Office	HMPO	Ad hoc
Department for Work & Pensions	DWP	Ad hoc
Driver & Vehicle Licensing Agency	DVLA	Ad hoc
UK VDBSs & Immigration	UKVI	Ad hoc
American Embassy	AE	Ad hoc
Security Industry Authority	SIA	Ad hoc

2. PURPOSE OF THIS DOCUMENT

2.1. What is a Privacy Impact Assessment?

Processes that involve exchanging or disclosing personal information inevitably give rise to privacy concerns. Indeed, the cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of corporations and Government agencies alike.

The PIA is a process mandated by Cabinet Office and recommended by the Information Commissioner which helps organisations to identify and address the likely privacy impacts of projects, in order that we can develop solutions, and ensure that concerns are addressed appropriately. For this reason we have undertaken a PIA for the R1 Project.

2.2. What does this PIA Report cover?

This report, whilst prompted by the R1 Project and the impact it will have on data collection, data sharing and processing, takes the opportunity to review all current incoming and outgoing data sharing arrangements that the DBS has in place with both internal and external stakeholders.

2.3. Maintenance of the Privacy impact assessment

The DBS aims to fulfil its roles and functions efficiently and effectively, maintaining a high quality delivery of services and products. Protection of an individual's privacy and the security of their personal information are fundamental to all that we do.

Given the possibility of changes in Government Legislation, and any future releases of the IT platform, this privacy impact assessment will be regularly reviewed.

2.4. How have we conducted the PIA?

We have sought to examine the arrangements both objectively and from the point of view of the individual, to ensure that we meet the legitimate expectations of those concerned. We believe that the arrangements that we have put in place reflect good practice in data sharing and protection, striking a fair balance between protecting the privacy rights of the individual and the protection of the public from risk of harm.

2.5. What type of PIA have we conducted?

In deciding whether to conduct a PIA, and what type of PIA to conduct, we considered carefully the nature and scope of the collection and disclosure of information to and from both internal and external stakeholders, and its potential to impact on the privacy rights of the individual, in particular that:

- information will be used by both the DBS and external stakeholders to make informed decisions with regards to the legal and suitability of employment of individuals

We also evaluated whether there was any immediate change to the collection and processing of the data, to assess the potential to impact on the privacy rights of the individual, in particular that:

- the DBS has two diverse functions that deliver the over arching objective of safeguarding children and vulnerable adults in the:
    - Disclosure Service
    - Barring Service

Currently the only anticipated changes to the processing of data previously collected by the DBS is the way in which it is transmitted, collected and stored will now primarily be electronic. On the basis of our assessment, we decided to follow a small scale PIA process.

The DBS will continue to utilise the security functions, processes and procedures put in place to protect the information previously implemented by the DBS and they will continue to conform to HMG Information Assurance Standards and Security Framework for the privacy and protection of data implementing upgrades as and when required to do so.

2.6. Is this report the end of the PIA process?

In consultation with partners, the DBS will closely monitor and review the scheme's operation, including ongoing review of the privacy impacts, and monitoring compliance with the specific privacy and security arrangements. This will help us ensure that the scheme continues to support the protection of the public from harm and provides benefits both to the DBS and our stakeholders.

3. DATA HANDLING

The DBS will only hold an individual's data if they have:

- Availed a DBS product (e.g. applied for a Disclosure check, subscribed to the Update Service, submitted a Barring referral, applied for a Barred List Check(BLC) or a Barred List Notification Subscription (BLNS);
- Been the subject of a DBS product (e.g. a Disclosure check, a Barring referral, or a BLC/BLNS).

The data we hold about individuals will be retained in line with the DBS Data Retention Policy (DRP) and is detailed in Appendix A.

The DBS cannot guarantee the security of information until it is in our possession, and will not take responsibility for such information until it has been received. However, one key benefit of the R1 project is that it will introduce a new secure

mechanism for organisations and individuals to submit data to DBS. This is described further in section 4.1.

Police and all other organisations that submit information to the DBS are responsible for transmitting the data via secure channels (by post or electronic means). DBS only takes responsibility for this data once it has been received by DBS. DBS has put in place secure methods for retaining and storing data. Incoming data received by the DBS is covered under the DBS Privacy Policy (DPP) which is published on the DBS website www.gov.uk/dbs.

The DBS is committed to being fully compliant with all relevant legislation including The Data Protection Act 1998 (DPA); The Safeguarding Vulnerable Groups Act 2006 (SVGA) and The Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 (SVGO) as well as other legislation, e.g. Police Act 1997, Human Rights Act 1998 etc, and have a legal duty to do so. The DBS takes all foreseeable precautions to protect the data in our possession.

The following principles will apply when we process any personal data:

- only data that is actually needed is collected and processed
- data is only seen by those who need it to carry out their jobs
- data is retained only for as long as it is required
- data is accurate and is only used as part of the DBS processes
- decisions are made on the basis of reliable and up to date data
- data is protected from unauthorised or accidental disclosure
- a person will be provided with a copy of data we hold on them, on request (DPA Section 7)
- there will be procedures in place for dealing promptly with any disputes / complaints
- data with regard to the Disclosure Service is only processed with a person's knowledge and consent

All of the above will apply whether we hold data on paper or in an electronic format.

3.1. Security of Data

DBS buildings have in place physical security measures to ensure appropriate access/egress; All DBS Staff are informed that any breach of the confidentiality agreement constitutes a breach of the Data Protection Act and may result in legal proceedings being brought against them;

- All DBS staff who have access to the data are subject to a minimum of Baseline Personnel Security Standard (BPSS) security clearance;
- All DBS staff undertake annual data protection training;
- All DBS staff's access to data is managed by Rules Based Access Controls (RBAC) (see also section 3.1.1) so as to enforce need to know principles;
- All documentation is evaluated as per HMG protective markings

3.1.1. Role Based Access Controls within the R1 System

The new R1 system introduces more rigorous RBACs for DBS users. The new system will be used by both Disclosure and Barring but the RBACs will ensure access is restricted to only the functionality, records and data users' need.

Access is restricted to users only being able to view case records and/or activities they have been allocated and are within their workload. It is further restricted to only allow users to access screens within the case records relevant to their role. Some of this access is also restricted to read-only access if that is required.

Only Managers defined within the RBACs hierarchy will be able to view their team's workloads. The audit history of a case is also restricted to a manager's view only.

Full access will be limited to Super-user type roles that will have the relevant security clearance and are very limited numbers.

The R1 system also allows users to 'discount' themselves from being allocated specific cases. This is used where there is a potential conflict of interest between the user and the subject of a case (e.g. family member, friend, neighbour etc).

3.2. Retention of data received

The DBS ensures that data is not held for longer than is necessary for its purpose. In establishing retention and archiving periods, the DBS make provision for barring case outcomes, patterns of behaviour established from repeat referrals, repeat disclosure applications, complaints and legal requirements. Further information is available in the DBS DRP.

To retain data indefinitely would contravene both the DPA 1998 and the Human Rights Act 1998. The DBS has a DRP in place to:

- Ensure the DBS only holds the information it needs to carry out its statutory functions and support the decisions it has made:
- Define the DBS's rationale for the retention of information;
- Ensure the integrity of the information is maintained;
- Ensure the information is only retained for as long as necessary in accordance with the law;
- Detail retention periods where a statutory retention period does not exist;
- Ensure that any information collected and held is proportionate in terms of the Human Rights Act 1998;
- Ensure information is accurate, relevant, kept up to date and held securely.

3.3. Storage of data

Personal data is held in secure computer files and, if required, paper files, which have restricted access. We have approved measures in place to stop unlawful access and disclosure.

We conduct regular compliance checks on all DBS departments and systems. All checks are to the standard set out by the Information Commissioners Office. In addition continuous security checks on our IT systems are undertaken.

DBS will ensure that any information collected and held is proportionate in terms of the Human Rights Act 1998 and ensure that it is accurate, relevant, kept up to date and held securely.

The new IT system will not invoke any changes to:

- Current data collection policies or practices;
- Current data quality assurance processes and standards;
- New or changed data retention arrangements.
- Ensure that any information collected and held is proportionate in terms of the Human Rights Act 1998

Before the introduction of R1, DBS Barring used paper case files. They were stored onsite when needed and stored in secure offsite storage facilities with TNT when closed. R1 brings the digitisation of paper case files but the use of the offsite storage facilities will remain until the paper case files are needed and retrieved for digitisation.

3.4. Other Data Uses

DBS uses the data it receives to perform its functions. To ensure the DBS is working as well as it can, it produces regular reports which are used internally and externally. The R1 system includes the Oracle Business Intelligence Enterprise Edition (OBIEE) software which provides the capability to perform analytics and reporting on the data.

DBS will use the OBIEE to monitor work in progress and completion targets for weekly, monthly and annual reporting. The OBIEE will also enable DBS Barring to analyse the data it has received to identify trends or areas for targeting. For example, DBS Barring will be able to produce statistics on which organisations or work groups refer individuals to DBS. Work can then be done to engage those stakeholders that do not make as many referrals as might be expected. It should be noted that such OBIEE reports will not make use of individuals' personal data but, will instead, collate generic volume data.

4. DATA SHARING

People are naturally concerned to ensure that there is an appropriate balance between the individual's right to privacy and the State's need to share data in order to carry out its functions effectively. People often have very different perspectives on where this balance should lie. The primary legal obligations are contained in the Data Protection Act 1998 and these are supplemented with other legislation requirements to share data.

Whilst the great majority of people agree that Government should share relevant data to an extent that is necessary and proportionate for their purposes – which is also the basic essence of UK data protection law – what this extent actually is in practical terms is often hotly debated.

Data sharing initiatives can therefore involve sharing a relatively substantial amount of data in order to find relevant nuggets within. Whether the data sharing is seen as justifiable is likely to depend on how many, and how valuable, those nuggets are, in comparison with the totality of the data sharing. The broader the data sharing, the more intrusive people will find it to be and the more value they will expect it to provide before they consider it to be justified.

It is therefore important for Government to ensure they target their activities to derive the maximum benefit for the public from the minimum data sharing, as a matter of public trust as well as legality.

Any data exchange between interested parties will take place over a secure accredited network to defend against interception during file transfer or via recorded delivery.

Any information that we may hold may be shared internally within the DBS to assist in the issue of Disclosure Certificates or to assist in the Barring Decision Making Process (BDMP). All information will continue to be held securely and will be shared only on a need to know basis.

4.1. DBS Online Services

A key benefit of the R1 system is the introduction of secure online services which enables various stakeholders to use a DBS online account to communicate and share data.

An internet version will serve most users, including private citizens applying for a Disclosure check or who are the subject of a Barring referral. The DBS website will act as a secure self-service interface and will provide customers with easy access to information, guidance and regularly updated Frequently Asked Questions (FAQs). A DBS online account will act as the primary channel for applications for DBS products and services.

An intranet version will also exist, primarily to service interactions with the Police and select other partner organisations (e.g. Disclosure Scotland (DS) and Access Northern Ireland (ANI)).

Access to online services will be subject to a rigorous and secure registration process, ensuring that all users are subject to the appropriate level of authentication, as determined by the products, services and data that they can access via this medium.

4.2. Alternative Delivery Mechanisms

If a recipient has chosen not to use the DBS online account or it is not appropriate, postal delivery will be used. Correspondence of a sensitive nature, such as those containing barred status information or copies of case papers, are all sent by special delivery to provide confidence that the correspondence has been delivered.

Special delivery enables a reference number known as the 'Track and Trace' number to be used on the Royal Mail website to confirm if, when and to whom correspondence has been delivered. Confirmation of the delivery status and, if available, a copy of the signature are retrieved from the website and stored in the case file.

Couriers may also be used by the DBS if information is of a highly sensitive nature or urgent delivery is required.

Although the preferred method of communication will be a DBS online account, there will be certain circumstances where this method is not appropriate and so the use of email will continue. Email will also be used within the interim period between DBS Barring R1 go-live and DBS Disclosure R1 go-live.

4.3. The Barred List Check and Barred List Notification Service

The Barred List Check (BLC) and Barred List Notification Service (BLNS) are brand new services that will be introduced in December 2016.

A BLC allows a one-off point-in-time check of the DBS barred lists to see if an individual is currently barred. This service will be available to Keepers of Registers (KoRs), Supervisory Authorities (SAs) and Regulatory Bodies (RBs) only.

A BLNS request enables requestors to register an interest in an individual and be notified in the event that that individual becomes barred on either barred list. This service will be available to KoRs and SAs only.

Both of these services will only be available online via a DBS online account and the results of these checks will only be published via the same means.

By the nature of the product, BLNS results are likely to be issued some time after the initial subscription is activated (if at all). Requestors therefore will have to reaffirm their eligibility to receive such personal information, by making a declaration at that time.

4.4. Contact Centre and Telephone Enquiries

DBS will be supported by the TCS Back Office and Contact Centre who will deal with first line enquiries from service users either by telephone or by white mail/scanned images. All TCS staff with either hold Baseline or Security Check (SC) clearance depending on their role however, all roles will be covered under the TCS RBACs.

TCS staff will follow the DBS Telephone Security Guidance Questions (TSQ) to verify the identity of the caller. They will be trained in answering only general telephone queries. They will not divulge any information to the caller regarding a case or whether a case is held, nor will they disclose the name of the person dealing with their case. If they are unable to answer a query, they will transfer the call to the onsite DBS Helpline Team. The DBS Helpline Team will also follow the TSQ before answering any telephone queries.

TCS staff will also have sight of / handle white mail and scanned images that will possibly relate to existing referral cases and have the ability to assign that documentation to an existing case or raise a service/information request within Siebel Customer Management System (CRM) for a caseworker to progress.

5. SUMMARY OF PRIVACY RISKS AND MITIGATION

The following sections show the results of the PIA analysis for each of the organisations that provide information to the DBS and those who DBS share information with.

5.1. Referring Parties

Referring parties can be any organisation that submits a barring referral to DBS.

a) Given the amount/type of data collected, what are the privacy risks? How might they be mitigated?

A referring party submits a referral to DBS Barring either online using a DBS online account, email or via post. A DBS online account provides a secure method for organisations to submit information to DBS as described in section 4.1. Therefore, if organisations use a DBS online account as their preferred method, the risks are mitigated.

An acknowledgement is sent to a referring party on receipt of a new referral or information for all referrals received either via the DBS online account or by post. This provides confirmation to the referring party that the information they have submitted has been received by the DBS.

The information contained in the referral includes nominal data relating to the referred individual, contact details for the referrer, details about the reasons for the referral and copies of relevant documentation the referring party deems relevant. In most cases each referral contains information relating to a single referred individual but may also contain information relating to more than one individual, victims and/or witnesses.

Section 35 of the SVGA imposes a duty on organisations to refer individuals to DBS e.g. Regulated Activity Providers (RAPs), and also lists the type of information that should be included as part of the referral, if such information exists. Local Authorities are given a power under Section 39 of the SVGA, to refer individuals to DBS.

All of the referral information is stored in the Customer Management System and is used to assess whether the referred individual should be barred from working with children and/or vulnerable adults. Compliance with HMG Security Framework and advised security controls are in place to protect our systems against attack i.e. hacking.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

The main use of the information received from a referring party is to support the consideration of the referred individual's suitability to work with children / vulnerable adults. If the referring party has submitted the referral using their DBS online account, the information they have submitted will be transposed straight into our system which reduces the risk of data inaccuracies due to re-keying of information.

The information can also be shared with other organisations, where legislation is in place and it is appropriate to do so, to enable those organisations to perform their relevant functions. Further assessment of the privacy risks can be found within the other relevant organisation's sections. Every referred individual is notified that information has been received by the DBS and how that information will be used including notification that the information may be shared with other relevant parties.

If a referral case meets a particular point (the Minded to Bar (MTB) point of internal processing), the DBS is required to enable the referred person to make comments as to why they should not be included in a Children or Adults' Barred List. The referred individual is provided with a copy of the case information that has been relied upon in coming to our consideration of MTB as required by the SVGA Schedule 3 Part 2 paragraph 16 (1) /SVGO Schedule1 Part 3 paragraph 16 (1). This information may have been provided by the referring party (as well as any other information collected from other organisations for the same purpose).

c) What are the risks associated with how long data is retained and how they might be mitigated?

Case papers and details received from a referring party are retained in accordance with the DBS' DRP as described in section 3.2. Data Retention is applied at the end of the case to ensure only the information we are required to retain is retained and where the next data retention review date is calculated to reconsider retention of data. Once the review date is reached, CRM creates a notification to the relevant team within DBS to ensure the next data retention review is undertaken. This ensures data is regularly reviewed so that it is not retained for longer than is necessary.

The system deletes all records that have been marked for a complete disposal and relevant individual papers that have been marked for deletion for a partial disposal in accordance with the current DBS DRP.

d) What are the privacy risks associated with internal sharing within the DBS and how they might be mitigated?

Security controls for the Home Office network are in place as per HMG Security Framework and standards to protect against attack.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

As described in section 5.1 (a). No further risks have been identified.

f) How could risks associated with individuals being unaware of the collection be mitigated?

To ensure transparency upon receipt of a referral, the Barring service issues a letter to the individual concerned to advise them that a referral has been received and is being considered and that the Barring service will contact them again once their further enquiries have been concluded.

Where the Barring service thinks it may be appropriate to bar, all information relied upon will be shared with the individual concerned and they will be given the opportunity to send representations for consideration. The information provided will

be redacted in certain circumstances for example, victim and witness details that are not to be disclosed.

g) What are the privacy risks associated with redress and how might they be mitigated?

All referred individual's can submit a Subject Access Request (SAR) under Section 7 of DPA and also copies of case information relied upon will always be provided to the referred individual if the case meets the MTB decision point as outlined in the SVGA Schedule 3 Part 2 Paragraph 16 (1)/ SVGO Schedule1 Part 3 Paragraph 16 (1).

As part of the Representation process, the referred individual can comment on whether they think the data is accurate. There are internal procedures to confirm if the data is incorrect and a process to correct it. If data recorded on CRM is incorrect, certain DBS users with the relevant access controls are able to amend the data. The previous data entry will be stored in the audit trail but only limited DBS roles will be able to view the audit.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

Only barring caseworkers and those that work on barring cases are able to access the barring information that has been allocated to a specific caseworker in the workflow. The case owner will use an escalation functionality to allow senior managers or experts to view case records to provide advice and guidance to progress the case. Further information on RBACs can be found in section 3.1.1.

All users that can view and access information provided at a higher level are restricted in numbers and security cleared to the relevant Home Office security level.

5.2. Referred Individuals

Referred individuals are the subjects of a barring referral. As part of the barring consideration process, they are provided with copies of all documentation that is being relied upon in the case and they can provide representations on why they should not be included in the children's and/or adults' barred list(s).

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

DBS Barring sends a copy of all the information DBS have relied upon to the referred individual, if the case reaches the Minded to Bar (MTB) stage, either online using their DBS online account or via postal special delivery depending on the referred individuals communication preference. This is known as a MTB bundle and can include the initial referral information and information gathered from other organisations (e.g. police, social services etc.). The referred individual uses this information to understand why they are being considered and also as a basis for them to provide their representations as outlined in SVGA Schedule 3 Paragraph 16 (1) /SVGO Schedule 1 Part 3 Paragraph 16 (1).

The referred individual provides DBS with representations which is information they believe will provide evidence/reasons why they should not be barred from working with children and/or adults. They are considered by DBS to aid in the final decision of whether the referred individual should be barred from working with children/vulnerable adults. Representations can be submitted either online using a DBS online account or via post.

A DBS online account provides a secure method for DBS to provide information to the referred individual and for them to submit information to DBS as described in section 4.1. Therefore, if the referred individual decides to use a DBS online account as their preferred method, the risks are mitigated.

An acknowledgement is sent to a referred individual on receipt of their representations received either via their DBS online account or by post. This provides confirmation to the referred individual that the information they have submitted has been received by the DBS.

Representations are stored in the CRM system. Security controls are in place for CRM to protect against attack i.e. hacking.

If a referred individual is subsequently barred, they have a right to request a review of the decision. If the Review request is submitted through their DBS online account the information will be transposed straight into our system which reduces the risk of data inaccuracies and incorrect matching to the existing referral due to re-keying of information.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

The MTB process of providing copies of the case information to the referred individual and them providing representations on why they should not be added to a barred list ensures the referred individual is aware of all of the information DBS

Barring has relied upon in their consideration of minded to bar and is given the opportunity to provide their reasons as to why they should not be included in a barred list.

Some referred individuals use the services of a solicitor or other representative to act on their behalf. Those referred individuals that have chosen to use a DBS online account can give their consent for a solicitor or representative to access the MTB bundle using their own registered DBS online account. Referred individuals can manage this access using the DBS online services to grant and remove this permission as needed.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Representations are retained in accordance with the DBS' Data Retention policy as described in section 3.2.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No further risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

Any MTB bundles that DBS issue are sent by post by special delivery. As described in section 4.2, the track and trace reference number is checked to confirm that the referred individual has received the letter and bundle.

For information relating to the DBS online services, see section 4.1.

If an individual is in prison, correspondence is sent via the prison governor or other named representative as agreed. The prison governor is asked to sign to confirm they have handed the correspondence to the prisoner. The prisoner is also asked to sign to confirm they have received the correspondence. A copy of these signatures is then sent to DBS Barring either in hard copy by post or a scanned copy by their DBS online account.

f) How could risks associated with individuals being unaware of the collection be mitigated?

No risks have been identified.

g) What are the privacy risks associated with redress and how might they be mitigated?

No risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

Only barring caseworkers and those that work on barring cases are able to access the barring information on CRM. The majority of cases will only be able to be accessed by the case owner through workflow. The case owner will use an escalation functionality to allow senior managers or experts to view case records and

provide advice and guidance in order to progress the case. Further information on RBACS can be found in section 3.1.1.

All users that can view and access the information provided by the referred individual are security cleared to the relevant Home Office security level.

5.3. Regulated Activity Providers

Regulated Activity Providers (RAPs) are defined in the SVGA Section 6/ SVGO Paragraph 10. They have a duty to refer individuals to the DBS if they have dismissed, or would have dismissed them had they not already left of their own accord, for safeguarding reasons. Therefore the PIA assessment for Referring Parties in section 5.1 (a – h) is also relevant for RAPs. This section will only detail any additional PIA risks and mitigation.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

No additional data is collected than that described in section 5.1 (a).

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional data is collected than that described in section 5.1 (b).

c) What are the risks associated with how long data is retained and how they might be mitigated?

No additional risks have been identified.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

Section 30A & 30B of the SVGA, when enacted, will provide legislation for specified individuals/organisations to request a BLC and BLNS on individuals. Information on these two services can be found in section 4.3. Theses services have been designed as ‘online only’ services.

Both of these services deliver results to those entitled to the information via the secure DBS online account only, which mitigates the risk.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Section 30A (4) & 30B (7) of the SVGA states that those entitled to request the information must also have the consent of the subject of the BLC and BLNS. The BLC and BLNS online request forms include a section for the requestor to declare that they have received the consent of the subject. Therefore, individuals will always be aware that barred status information has been provided to the requestor.

g) What are the privacy risks associated with redress and how might they be mitigated?

BLC and BLNS subjects are able to dispute barred status information if they believe it is incorrect. This follows the same disputes process as the one used in Disclosure.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.4. Police

DBS request information from the police under Section 50A of the SVGA on referrals where further police information is required. This information is specific relevant pieces of information such as ages of victim to requests for copies of police files.

The police can also request information from DBS under Section 50A of the SVGA to aid in their investigations and prosecutions, for safeguarding purposes and for police vetting and recruitment purposes and any prescribed purpose. The DBS must, provide to any chief officer of police a barred list or information as to whether a particular person is barred. For the purposes of the protection of children or vulnerable adults, DBS must provide to a relevant authority any information which DBS reasonably believes to be relevant.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

DBS Barring will use an intranet DBS online account to request and receive police information for barring purposes. The Disclosure Units in Local Police Forces (LPFs) will receive the requests and provide the response. Police information can also be sent by post in certain circumstances e.g. documentation is too large, hard media is being provided.

Police information can include specific offence details e.g. age of victim, location of offence, updates on police investigations or prosecutions, or copies of police information/documents such as summaries, witness statements, police interviews etc.

A DBS online account provides a secure method for the police to submit information to DBS as described in section 4.1.

SVGA, POFA and an MOU provide provisions for DBS to request and receive the information from the police.

All of the police information is stored in CRM and is used to consider whether the referred individual should be barred from working with children and/or vulnerable adults. HMG Security Framework and advised security controls are in place to protect our systems against attack i.e. hacking.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

The main use of the information received from the police is to support the consideration of the referred individual's suitability to work with children / vulnerable adults. A DBS online account allows certain specific information to be transposed straight into our system which reduces the risk of data inaccuracies due to re-keying of information.

The Oracle Business Intelligence Enterprise Edition (OBIEE) software will be used to produce Management Information (MI) on case statistics and responses to and from

the police. The responses MI will be used to target police forces that are not sending responses back in a timely manner. For further information on the OBIEE please see section 3.4.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Police information is retained in accordance with the DBS' DRP as described in section 3.2.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

The police can request information from DBS using Section 50A of SVGA, Article 52A of the SVGO and DPA Section 29(3), to aid their investigations and prosecutions, for safeguarding purposes or for police vetting and recruitment or a prescribed purpose.

The information provided to the police can include barred statuses, case outcomes and copies of referral papers.

All requests from the police for information will be submitted and responded to using a DBS online account. Further information on the DBS online services can be found in section 4.1.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Information responses from the police become part of the case processing. Whilst considering a case, the referred individual is notified that the DBS may share information with other parties if required and legislation permits DBS to do so.

Information will be redacted in circumstances for example, victim details that are not to be disclosed. If the police do not give permission for data they have provided to be disclosed, the information will not be considered in the decision.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

In addition to the risks and mitigation discussed in section 3.1.1, only specific users will be able to view the police request records. No other users will be able to access the police request records unless they have a legitimate business reason to do so.

5.5. PNC

Information from PNC is utilised in the discretionary decision making and Autobar processes within Barring and is received in two forms. The first is a daily extract that contains nominal, caution and conviction data that is imported into the system and utilised when matching records. The second is live PNC access from dedicated terminals to obtain further information whenever necessary. This is tightly controlled through RBACs and external PNC auditing.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

Access to live PNC data by Barring Operations is via dedicated terminals and is covered by PNC Syops and NPIA Data Sharing Agreement as this is police sharing data with DBS.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Police information is retained in accordance with the DBS' Data Retention policy as described in section 3.2

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

No additional risks have been identified.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Information obtained from PNC becomes part of the case and will be provided to the individual if a decision to bar is reached, additionally where a decision to bar is not reached the individual may still submit a Subject Access Request (SAR) under Section 7 of the DPA to obtain all data the DBS currently holds on them.

Whilst considering a case, the referred individual is notified that the DBS may share information with other parties if required and legislation permits DBS to do so.

Information will be redacted in circumstances for example, victim details that are not to be disclosed. If the police do not give permission for data they have provided to be disclosed, the information will not be considered in the decision.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified. Further information in relation to the dispute of PNC information any possible redress will be covered within the Disclosure PNC section.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.6. PLX

The Police Local Cross-Referencing System (PLX) is a data source containing nominal details of local records held by police forces. The PLX interface is used in both Disclosure and Barring.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

In Barring, all new referrals are matched against PLX to identify which, if any, police forces hold information in relation to the referred individual. PLX only contains nominal information about an individual e.g. name, date of birth etc, and the name of the LPF that holds the information. If DBS Barring require this information the LPF holds, they will send a request through a DBS online account to the LPF. This is covered in the Police PIA assessment in section 5.4 (a – h).

The PLX interface is stored in accordance with HMG Security framework and advised security controls to protect our systems against attack i.e. hacking.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

No additional risks have been identified.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

No additional risks have been identified.

f) How could risks associated with individuals being unaware of the collection be mitigated?

No additional risks have been identified.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.7. PND

Sharing the barred lists with Police National Database (PND) satisfied the legislative requirement brought in by Section 50A of the SVGA to provide the barred lists to the police.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

DBS Barring upload barred status and nominal information direct to PND via a secure PSN terminal on a weekly basis. A reconciliation file is received from PND which is validated through an access database to ensure all has been uploaded correctly.

Specific PND Users will have access to the markers set on the PND Database to inform the police of the individuals 'Barred Status'. This is mitigated with the Role Based Access Controls to PND, all requests for PND information are authorised by a Supervisor and all PND access is audited.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

The markers set on PND will remain in place as long as the individual is on a DBS Barred List (The bar is for life, subject to appeal or review). If an individual is removed from a DBS Barred List(s) the PND Marker will be removed accordingly.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

Work was undertaken to identify the potential risk of other agencies with access to PND accessing barred status information. This was mitigated by security controls, limiting the data to Data Access Restriction Coding (DARC) level 5 users on PND and adding a security prompt to confirm eligibility to view information. PND record access is also heavily audited and controlled.

f) How could risks associated with individuals being unaware of the collection be mitigated?

No additional risks have been identified.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

The existing access and security controls within PND are sufficient for access to the DBS barred markers.

5.8. Home Office PNC Services

Police National Computer Services (PNCS) provide DBS with a monthly extract of PNC data, which contains nominal and offence details of individuals who have been cautioned or convicted of a specified (potential) Autobar offence.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

The data is sent by email, over the secure .gsi network. DBS staff log onto a PGP (Pretty Good Privacy) network to retrieve the email. A password is required to access the data, which is supplied separately by PNC.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

PNC information is retained in accordance with the DBS' DR policy as described in section 3.2

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

No additional risks have been identified.

f) How could risks associated with individuals being unaware of the collection be mitigated?

No such risk exists as all individuals cautioned or convicted of an Autobar offence are informed that the offence may be notified to the DBS for safeguarding purposes.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.9. Access Northern Ireland

Access Northern Ireland (ANI) is the criminal history disclosure service in Northern Ireland and operates under Part V of the Police Act 1997. DBS Barring considers whether individuals should be barred from working with vulnerable groups on behalf of Northern Ireland using the SVGO.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

POFA Part 5 Chapter 1 paragraph 67 (2) amended the SVGA which as a consequence changed the barring powers of the DBS, in cases other than those meeting the criteria for automatic inclusion without the right to make representations, require the DBS to be satisfied that it has reason to believe that the individual under consideration "is or has been or might in future be engaged in regulated activity". This is internally referred to as the Test for Regulated Activity (TRA). One of the evidence sources of TRA is whether the individual has applied for a disclosure check for work in regulated activity which includes certain disclosure checks carried out by ANI.

All new referrals (unless TRA has already been satisfied) will be checked with ANI to see if they have any evidence of a disclosure check. This will be undertaken automatically by the system using a Web service. This is a secure service that mitigates the risks of sharing information back and forth between DBS and ANI.

At R1 phase 2 go-live, ANI will begin offering the Disclosure Update Service to their customers. Therefore DBS Barring will begin receiving referrals from ANI where individuals have submitted a disclosure check and/or are members of the Update Service, which contain relevant criminal or police information that the Police feel should be considered by DBS. These referrals are known as Disclosure Information Team (DIT) referrals.

ANI DIT referrals will be sent to DBS Barring via an interface based on Secure File Transfer Protocol (SFTP) mechanism over the secure CJX network. This is a secure interface which has the relevant HMG Security Framework and advised security controls in place.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

DBS and ANI share a range of sensitive information to enable both organisations to perform their duties. The SVGO Schedule 1 Para 21 provides for daily files to be provided to ANI on behalf of the NI Secretary of State. There is also an MOU in place that shows the agreements on how the data will be handled.

The ANI DIT referrals received through the interface will be transposed straight into our system which reduces the risk of data inaccuracies due to re-keying of information.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Any information from ANI including TRA evidence and DIT referrals are retained in accordance with the DBS' DR policy as described in section 3.2.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

ANI uses the DBS Barring lists to process disclosures. SVGO Schedule 1 Para 21 provides legislation for daily files, to be provided to ANI on behalf of the NI Secretary of State. Two files containing nominal details of those individuals that are barred from working with children and vulnerable adults are sent daily to ANI via an interface based on SFTP mechanism over the secure CJX network. This is a secure interface which has the relevant HMG Security framework and advised security controls in place.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Referred individuals are informed in correspondence from DBS Barring that information will be shared with other relevant organisations where legislation permits DBS to do so.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

The ANI interface and web service will run on schedules without the need for user intervention (unless an issue occurs).

5.10. Disclosure Scotland

Disclosure Scotland (DS) is an Executive Agency of the Scottish Government operating on behalf of Scottish Ministers. They provide a criminal history disclosure service in Scotland and make barring decisions on behalf of the Scottish Government. Scotland derives it's barring powers from the Protection of Vulnerable Groups (Scotland) Act 2007.

Legislation is in place in Part 5 Chapter 1 paragraph 74 (1) and Schedule 3 Part 1, Paragraph 6 of the SVGA to ensure that if a bar that has been placed on an individual by DS it is recognised in England, Wales and Northern Ireland and a bar made by DBS is recognised in Scotland. Schedule 3 part 1 paragraph 6 provides that we must not consider the individual on the children's list if they have already been considered on a corresponding list by DS. Schedule 3 Part 2 paragraph 12 provides the same for adults.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

DBS use a number of interfaces and processes to ensure that individuals are not considered by both DBS and DS. This ensures that where possible the DBS and DS schemes work closely together and make decisions that are cohesive (i.e. avoiding two different organisations considering the same information and potentially coming to a different decision and preventing double barring).

DBS uses the DS Barring lists to process disclosures and to determine if DS have already barred an individual. A file containing nominal details of those individuals that have been barred from working with children and vulnerable adults since the last file is sent daily to DBS via an interface based on SFTP mechanism over the secure CJX network. This is a secure interface which has the relevant HMG Security Framework and advised security controls in place.

DS will also provide DBS with a list of individuals they are currently considering. This list will be a file containing nominal details of those individuals that are being considered since the last file was sent daily to DBS via an interface based on SFTP mechanism over the secure CJX network. This is a secure interface which has the relevant HMG Security Framework and advised security controls in place.

All new referrals will be automatically checked by the system against these lists.

The interfaces will not by ready by R1 Barring go-live and so an interim process has been developed. An extract of the DBS Barring lists will be emailed to DS using secure email. DS will then acknowledge they have received the email.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

DBS will ask DS if they have previously considered an individual, and ask if DS has registered an individual in the DS scheme which is evidence they satisfy TRA (For more information on TRA see section 5.9 (a)). DBS can also ask DS for copies of any case information they may hold. The request and response will be submitted

using a DBS online account or by email or post if necessary. Further information on DBS online services can be found in section 4.1.

TCS have confirmed that DS will not be ready in time to begin using a DBS online account for R1 Barring go-live. Therefore an interim process has been developed where DBS and DS will utilise secure email. DBS will then acknowledge they have received the email response.

All of the information from DS is stored in CRM and is used to consider whether the referred individual should be barred from working with children and/or vulnerable adults. HMG Security Framework and advised security controls are in place to protect our systems against attack i.e. hacking.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Any information from DS is retained in accordance with the DBS' Data Retention policy as described in section 3.2.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

DS uses the DBS Barring lists to process disclosures and to determine if DBS have already barred an individual. Schedule 3, Part 3, Paragraph 22A of the SVGA enables DBS to provide barred list information to DS. A file containing nominal details of those individuals that have been barred from working with children and vulnerable adults since the last file is sent daily to DS via an interface based on SFTP mechanism over the secure CJX network. This is a secure interface which has the relevant HMG Security Framework and advised security controls in place.

DS will ask DBS if they have previously considered an individual for barring. DS can also ask DBS for copies of any case information they may hold. The request and response will be submitted using their DBS online account or by secure email or post if necessary. Further information on the DBS online services can be found in section 4.1.

TCS have confirmed that DS will not be ready in time to deliver the DS interfaces for R1 Barring go-live. Therefore an interim process has been developed where DBS and DS will utilise secure email. DS will then acknowledge they have received the email response.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Referred individuals are informed in correspondence from DBS Barring that information will be shared with other relevant organisations where legislation permits DBS to do so.

g) What are the privacy risks associated with redress and how might they be mitigated?

The processes described above should prevent double barring which will avoid the situation where an individual could request an appeal from two different tribunals.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

The DS interfaces will run on schedules without the need for user intervention (unless an issue occurs).

5.11. Keepers of Registers

Keepers of Registers (KoRs) are defined and listed in Section 41 (7) of the SVGA. This section covers the PIA assessment for all the KoRs. Any risks and mitigation relating to information specific to a KoR can be found in the relevant section.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

KoRs have the power to refer individuals to DBS. As a referring party the risks and mitigation described in the Referring Parties section at 5.1 are all relevant for KoRs.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

Barring Operations have MoUs in place for the majority of KoRs and no additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Information from a KoR is retained in accordance with the DBS' DRP as described in section 3.2.

Each KoR will have its own Data Retention Policy to adhere to.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No risks identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

Section 43 of the SVGA makes provision for KoRs to request barred information in respect of individuals that are included on or being considered for inclusion on their register. The SVGA also enables DBS to proactively provide information to a KoR if it is relevant to their function and otherwise appropriate to provide.

To enable DBS Barring to identify individuals on a register that are subsequently barred, KoRs will register all those individuals with the BLNS service from go-live. Using the BLNS service will ensure KoRs are notified straight away if any of their individuals are subsequently barred. Before an organisation is notified of such a bar, the BLNS process requires that they complete a declaration to affirm that they still have an interest in the individual, ensuring that barred information is only being shared appropriately.

KoRs can also use the BLC service for barred list checks. Further information on the BLC and BLNS can be found in section 4.3. These services have been designed as 'online only' services.

Other information that could be shared with a KoR could be barring case outcomes (no action outcomes) and/or copies of redacted case information. Information would be provided either using a DBS online account or by post using special delivery.

Both delivery methods provide secure measures. Further information can be found at section 4.1 for the DBS online services and section 4.2 for postal methods.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Referred individuals are informed in correspondence from DBS Barring that information may be shared with other relevant organisations where legislation permits DBS to do so.

g) What are the privacy risks associated with redress and how might they be mitigated?

BLC and BLNS subjects are able to dispute barred status information if they believe it is incorrect. This follows the same disputes process as the one used in Disclosure.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.12. Supervisory Authorities

Supervisory Authorities (SAs) are defined within Section 45(7) of the SVGA. A full list of all the SAs can be found at Appendix C.

This section covers the PIA assessment for all the SAs. Any risks and mitigation relating to information specific to a SA can be found in the relevant section.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

SAs have the power to refer individuals to DBS. As a referring party the risks and mitigation described in the Referring Parties section at 5.1 are all relevant for SAs.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

Barring Operations have MoUs in place for the majority of SAs and no additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Information from an SA is retained in accordance with the DBS' Data Retention policy as described in section 3.2.

Each SA will have its own Data Retention Policy to adhere to.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

Sections 45 (7) 46, 47, 48, & 49 of the SVGA provides provision for SAs to request barred information in respect of certain individuals. Section 50 of the SVGA also enables DBS to proactively provide information to a SA if the DBS thinks that it is relevant.

To enable DBS Barring to identify individuals that a SA may have an interest in and that are subsequently barred, SAs will register all those individuals with the BLNS service from go-live. Using the BLNS service will ensure SAs are notified straight away if any of their individuals are subsequently barred. Before an organisation is notified of such a bar, the BLNS process requires that they complete a declaration to affirm that they still have a legitimate interest in the individual, ensuring that barred information is only being shared appropriately.

SAs can also use the BLC service for barred list checks. Further information on the BLC and BLNS can be found in section 4.3. These services have been designed as 'online only' services.

Other information that could be shared with an SA could be barring case outcomes (no action outcomes) and/or copies of redacted case information. Information would

be provided by either using their DBS online account or by post using special delivery. Both delivery methods provide secure measures. Further information can be found at section 4.1 for the DBS online services and section 4.2 for postal methods.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Referred individuals are informed in correspondence from DBS Barring that information may be shared with other relevant organisations where legislation permits DBS to do so.

g) What are the privacy risks associated with redress and how might they be mitigated?

BLC and BLNS subjects are able to dispute barred status information if they believe it is incorrect. This follows the same disputes process as used by DBS Disclosure.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.13. National College for Teaching and Leadership

The National College for Teaching and Leadership (NCTL) is a SA that looks after individuals working within the Education sector in England. This includes teachers, teaching assistants etc., therefore the PIA assessment for SAs in section 5.12 (a – h) is also relevant for the NCTL. This section will only detail any additional PIA risks and mitigation.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

NCTL inform DBS of their Prohibition Orders and strike offs. These notifications will be made through a DBS online account or by post if needed.

NCTL also send a monthly list of cases they are considering. This enables DBS to confirm that NCTL still have a valid interest in these individuals which reduces the risk of sharing information with NCTL that they should not have.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified here.

c) What are the risks associated with how long data is retained and how they might be mitigated?

As described in section 3.2. No further risks have been identified.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

DBS Barring holds an MoU with the NCTL. If DBS Barring identifies that the referral involves a person in education, a copy of the referral documents are sent to the NCTL so that they can perform their own professional misconduct proceedings. An End of Case notification (EoC) record is also created on the barring case record. This ensures that when the barring case is concluded, NCTL are notified of the case outcome. Only no action results need to be communicated to NCTL in this way as bars will be notified using the BLNS service as described in section 15.12 (e).

If the case outcome is no action, NCTL are sent a list of the documentation held along with the 'no action' notification. NCTL can then check this list to see if they require any of this information. This ensures that information issued is proportionate to the requirement.

Documents that could be sent to NCTL only include the initial referral and some subsequent information that has been gathered. DBS do not share police information, court findings, medical reports, specialist risk assessments, information not to be shared without consent or the referred individual's representations with the NCTL as this information has only been provided to DBS for their purpose. On some

occasions the referred individual's representations can be sent to the NCTL if the referred individual asks for them to be.

Information is sent by DBS either using a DBS online account or by post using special delivery. Both delivery methods provide secure measures. Further information can be found at section 4.1 for the DBS online services and section 4.2 for postal methods. If the documents are sent by post, a list of the documents is included with the bundle and NCTL are asked to validate the list against the contents to ensure no documents have gone missing.

f) How could risks associated with individuals being unaware of the collection be mitigated?

An individual who is registered with the NCTL is advised in writing by DBS that the NCTL will be informed of the outcome of the case whatever decision has been reached.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.14. Education Workforce Council

The Education Workforce Council (EWC) was previously known as the General Teaching Council for Wales (GTCW). EWC is a KoR that includes teachers, lecturers in Further Education and Further Education Support Workers, therefore the PIA assessment for KoRs in section 5.11 (a – h) is also relevant for the EWC. This section will only detail any additional PIA risks and mitigation.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

The EWC inform DBS of any of their misconduct cases that result in a bar from working in education. These notifications will be made through a DBS online account or by post if needed.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

As described in section 3.2. No additional risks have been identified.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

DBS Barring holds an MoU with the EWC. If DBS Barring identifies that EWC holds a record of a referred individual, an End of Case notification (EoC) record is created on the barring case record. This ensures that when the barring case is concluded, EWC are notified of the case outcome. Only no action results need to be communicated to EWC in this way as bars will be notified using the BLNS service as described in section 15.12 (e).

If the case outcome is no action, EWC are sent a copy of documents that could include the initial referral and some subsequent information that has been gathered. DBS do not share police information, court findings, medical reports, specialist risk assessments, information not to be share without consent or the referred individual's representations with the EWC as this information has only been provided to DBS for their purpose. On some occasions the referred individual's representations can be sent to the EWC if the referred individual asks for them to be.

Information is sent by DBS either using a DBS online account or by post using special delivery. Both delivery methods provide secure measures. Further information can be found at section 4.1 for the DBS online services and section 4.2 for postal methods. If the documents are sent by post, a list of the documents is included with the bundle and EWC are asked to check the list against the contents to ensure no documents have gone missing.

f) How could risks associated with individuals being unaware of the collection be mitigated?

An individual who is registered with the EWC will be advised in writing by DBS that the EWC will be informed of the outcome of the case whatever decision has been reached.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.15. General Teaching Council for Northern Ireland

The General Teaching Council for Northern Ireland (GTCNI) is a KoR that includes teachers in Northern Ireland under Article 43 (7) of the SVGO.

Therefore the PIA assessment for KoRs in section 5.11 (a – h) is also relevant for GTCNI. This section will only detail any additional PIA risks and mitigation.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

GTCNI inform DBS of any of their misconduct cases that result in a bar from working in education. These notifications will be made through a DBS online account or by post if needed.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

As described in section 3.2. No additional risks have been identified.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

If DBS Barring identify that a referred individual is registered with GTCNI, an End of Case notification (EoC) record is created on the barring case record. This ensures that when the barring case is concluded, GTCNI are notified of the case outcome. Only no action results need to be communicated to GTCNI in this way as bars will be notified using the BLNS service as described in section 15.12 (e).

If the case outcome is no action, GTCNI are sent a copy of documents that could include the initial referral and some subsequent information that has been gathered. DBS do not share police information, court findings, medical reports, specialist risk assessments, information not to be share without consent or the referred individual's representations with GTCNI as this information has only been provided to DBS for their purpose. On some occasions the referred individual's representations can be sent to GTCNI if the referred individual asks for them to be.

Information is sent by DBS either using a DBS online account or by post using special delivery. Both delivery methods provide secure measures. Further information can be found at section 4.1 for the DBS online services and section 4.2 for postal methods. If the documents are sent by post, a list of the documents is included with the bundle and GTCNI are asked to check the list against the contents to ensure no documents have gone missing.

f) How could risks associated with individuals being unaware of the collection be mitigated?

An individual who is registered with GTCNI will be advised in writing by DBS that GTCNI will be informed of the outcome of the case whatever decision has been reached.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.16. Tribunals – Barring Appeals (Upper Tribunal, Care Tribunal)

If an individual is included on a barred list, they have a right to Appeal the barring decision within 3 months of the date of the DBS' decision. The barred individual submits their request for an appeal to the relevant Tribunal. Appeals for England and Wales are dealt with by the Upper Tribunal and appeals for Northern Ireland are dealt with by the Care Tribunal.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

When a barred individual submits an application for Permission to Appeal the relevant Tribunal, under the Tribunal rules, will provide a copy of the Appellant's Permission to Appeal application to DBS. This will include information from the appellant which may consist of statements and/or other evidence to support the appellant's appeal. This information can either be submitted through a DBS online account or by post.

Should the Tribunal decide to use a DBS online account to submit the appeal, they can use the online appeal form and the information they have submitted will be transposed straight into our system which reduces the risk of data inaccuracies and incorrect matching to the existing referral due to re-keying of information.

All appeal information is used by specified DBS users, the relevant Tribunal and other involved parties as part of the appeal process.

All of the appeal information is stored in the system. HMG Security framework and advised security controls are in place to protect our systems against attack i.e. hacking.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

The information provided is shared in accordance with Tribunal Rules. The information is utilised by the allocated Tribunal Judge to enable any decisions to be made in respect of any material error of fact or error of law in the DBS' decision. The information is also provided to the appellant within the proceedings.

All parties involved in the hearing, bring a hard copy of the information when they attend the hearing. The DBS case files are kept in locked brief cases which remain in the caseworker's possession at all times.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Appeal documentation is retained in accordance with the DBS' Data Retention policy as described in section 3.2.

The Tribunals are subject to their own policies and procedures.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

On receipt of the Permission to Appeal application, DBS Barring will provide copies of all the case information relied upon in the barring decision to the Tribunal either through a DBS online account or by post using special delivery. The case information includes the initial referral information, information gathered from other organisations (e.g. police, social services etc), the individual's representations and the BDMP document which is an extract of the relevant assessment and decision fields from the case record.

Any appeal information sent by post is sent by special delivery. As described in section 4.2, the track and trace reference number is checked to confirm that the referred individual has received the letter.

For information relating to DBS online services, see section 4.1.

f) How could risks associated with individuals being unaware of the collection be mitigated?

No additional risks have been identified.

g) What are the privacy risks associated with redress and how might they be mitigated?

The Appeal Hearing is attended by specified DBS colleagues and the appellant. During the hearing inaccuracies can be challenged i.e. material error of fact or errors of law.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

In addition to the risks and mitigation discussed in section 3.1.1, only specified DBS users will be able to view appeal case records. No other users will be able to access appeal records unless they have a legitimate business reason to do so.

5.17. National Assembly for Wales

The National Assembly for Wales (commonly known as the Welsh Assembly) receive relevant details of individuals that have been referred to the DBS who live and/or work in Wales. The Welsh Assembly has a number of different functions in relation to education, health and social care.

The Welsh Assembly can refer individuals to the DBS, therefore the PIA assessments for Referring Parties in section 5.1 (a – h) and RAPs in section 5.3 (a – h) are also relevant for the Welsh Assembly. This section will only detail any additional PIA risks and mitigation.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

No additional risks have been identified.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

No additional risks have been identified.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

If DBS Barring identify that a referred individual lives or works in Wales, an EoC record is created on the barring case record. This ensures that when the barring case is concluded, the Welsh Assembly are notified of the case outcome.

The Welsh Assembly can also request barred information on individuals they have a valid interest in knowing about using a DBS online account or by post. Information would be provided either using their DBS online account or by post using special delivery. Both delivery methods provide secure measures. Further information can be found at section 4.1 for the DBS online services and section 4.2 for postal methods.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Individuals are advised in writing by DBS that the Welsh Assembly will be informed of the outcome of the case whatever decision has been reached if appropriate.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.18. Local Authorities

Local Authorities (LAs) also include Child and Adult Social Services and Local Authority Designated Officers (LADOs).

LAs have a power under Section 39 of the SVGA to refer individuals to the DBS if they have dismissed or would have dismissed them due to safeguarding concerns. Therefore the PIA assessment for Referring Parties in section 5.1 (a – h) is also relevant for LAs. This section will only detail any additional PIA risks and mitigation.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

DBS can request additional case information under Section 40 of the SVGA from LAs to support a referral. The request and the response can either be sent through a DBS online account or by post depending on the LAs preferred contact method.

The response can include information about the circumstances of the referral, copies of strategy meeting minutes etc.

All of the additional case information from an LA is stored in the Customer Management System and is used to consider whether the referred individual should be barred from working with children and/or vulnerable adults. HMG Security framework and advised security controls are in place to protect our systems against attack i.e. hacking.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

The main use of the information received from an LA is to support the consideration of the referred individual's suitability to work with children / vulnerable adults. Section 40 of the SVGA enables DBS to request and receive additional case information from the LA.

A DBS online account provides a secure method for DBS to provide information to an LA and for them to submit information to DBS as described in section 4.1. Therefore, if the LA decides to use a DBS online account as their preferred method, the risks are mitigated.

DBS are aware that some LADOs request the outcome of cases that the LA has referred to DBS. DBS are very vigilant with regard to this and always ensure that if a request for a case outcome is received, the requestor has a valid legitimate interest in knowing the result before they release any information.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Information from an LA is retained in accordance with the DBS' DRP as described in section 3.2.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

No additional risks have been identified.

f) How could risks associated with individuals being unaware of the collection be mitigated?

No additional risks have been identified.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.19. National Offender Management Service

The National Offender Management Service (NOMS) is an executive agency that manages individuals that have been given sentences and orders by courts.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

Most information sharing is initiated by a request from NOMS. There are circumstances though, either following a request or not, where DBS request nominal information from NOMS e.g. current address. The request and the response should be submitted through a DBS online account although a postal route has also been designed as an alternative.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

NOMS requests are retained in accordance with the DBS' DRP as described in section 3.2.

NOMS are subject to their own policies and procedures.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

NOMS will initiate requests for information through their DBS online account. They require this information for potential placements/training to ensure the individual is suitable to work with specific offenders. NOMS can request information under Section 50A of the SVGA.

Responses to NOMS requests are sent using their DBS online account or by post. The response can include whether a particular individual is barred or not and/or any information which DBS reasonably believes to be relevant.

If DBS have received a request from NOMS for information and do not have a referral for the subject, DBS request a PNC and check to see if the offence is relevant and if so refer to Autobar for consideration.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Whilst considering a case, the referred individual is notified that the DBS may share information with other parties if required and legislation permits DBS to do so.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

In addition to the risks and mitigation discussed in section 3.1.1, only specified DBS users will be able to view the NOMS request records. No other users will be able to access the NOMS request records unless they have a business reason to do so.

5.20. National Probation Service

The National Probation Service (NPS) is responsible for offenders once they have been released from prison.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

Most information sharing with the NPS is initiated by a request from them under SVGA Section 50A section 1(b) & (c). There are circumstances though, either following a request or not, where DBS request nominal information from the NPS e.g. current address.

The request and the response from/to the NPS should be submitted through a DBS online account although a postal route has also been designed as an alternative. This alternative has been designed specifically with the NPS in mind as it is currently being tendered out to private Community Rehabilitation companies.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

NPS requests are retained in accordance with the DBS' DRP as described in section 3.2.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

The NPS will send requests for information through their DBS online account or by post. They require this information for potential placements/training to ensure that an individual is suitable to work with specific offenders. They can request information using Section 50A 1(b) & (c).

Responses to NPS requests are sent using their DBS online account or post. The response can include whether a particular individual is barred or not and/or any information which DBS reasonably believes to be relevant.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Whilst considering a case, the referred individual is notified that the DBS may share information with other parties if required.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

In addition to the risks and mitigation discussed in section 3.1.1, only specified DBS users will be able to view the NPS request records. No other users will be able to access the NPS request records unless they have a legitimate business reason to do so.

5.21. Department for Education

The Department for Education (DfE) is responsible for the education and children's services in England. They liaise with DBS in relation to the pension scheme for teachers under SVGA Schedule 3, Part 3 Paragraph 21 and Teachers Pensions Regulations 2010 Schedule 7, Paragraph 4.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

No additional risks have been identified.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

No additional risks have been identified.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

Schedule 3, Part 3 Paragraph 21 of SVGA makes provision for the Teachers Pensions department in DfE to request information on barred individuals who have a teacher's pension. DfE require this information to determine whether a teacher claiming their pension on ill health is claiming to avoid being disciplined for a safeguarding concern as in these circumstances DfE will refuse the application.

To enable DBS Barring to identify individuals with a teacher's pension that are subsequently barred, DfE will register all those individuals with the BLNS service from go-live. Using the BLNS service will ensure DfE are notified straight away if any of their individuals are subsequently barred. Before an organisation is notified, the BLNS process ensures that the organisation still has a legitimate interest in that person. This ensures organisations are only given barred information if they need it. Further information on the BLNS can be found in section 4.3.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Whilst considering a case, the referred individual is notified that the DBS may share information with other parties if required and legislation allows DBS to do so.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

See section 3.1.1. No additional risks have been identified.

5.22. Specialist Risk Assessors

Specialist Risk Assessments (SRAs) are contracted by DBS on a case by case basis dependant upon the 'speciality' risk assessment that is required. Some SRAs are contracted to companies e.g. Lucy Faithful Foundation and some are sole traders.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

DBS issues a request for quotation to the SRAs to commission a specialist assessment report. Once contracts have been agreed, redacted copies of the case papers (which can include the initial referral information, information gathered from other organisations e.g. police, social services etc. and any representations submitted by the referred individual) are issued to the SRA using a DBS online account or by post.

The SRA uses the redacted case information to understand the circumstances of the referral and as a basis for conducting interviews with the referred individual to produce a specialist assessment report.

The report is stored in the CRM system. HMG Security Framework and Security controls are in place for CRM to protect against attack i.e. hacking.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

The report is considered by DBS to aid in the decision of whether the referred individual presents a potential risk to children and /or vulnerable adults.

A copy of the report is sent to the referred individual in order for them so that they can comment on the report and state whether they think anything is inaccurate.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Risk assessment reports will be retained in accordance with the DBS DRP.

SRAs are informed of all the security requirements they need to conform with and provide evidence to DBS of the compliance prior to any information being issued to them. They return all paperwork or files and confirm they have deleted all electronic records to the required security standards in relation to subjects the DBS are considering for barring after 6 months from the filing of the reports. The return paperwork is validated against what was issued and then securely destroyed by DBS.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No further risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

The first initial contact with the SRA includes a summary but contains no identifying personal data.

The DBS online services have built in security measures. Requests and reports sent by post are sent by special delivery.

f) How could risks associated with individuals being unaware of the collection be mitigated?

The referred individual is asked to consent to a report being commissioned. Although they can decide not to give their consent for an interview based report, they are informed that DBS may still provide information and commission a paper based only report.

If the case is not at MTB stage the SRA is advised that they can not share the information with the referred individual. The referred individual is sent a separate bundle of papers which is redacted to SAR standard as per Section 7 of the DPA.

g) What are the privacy risks associated with redress and how might they be mitigated?

A copy of the report is always provided to the referred individual. If a referred individual provides comments saying the contents of the report are incorrect, in relevant circumstances, the SRA is contacted and they can agree/disagree to provide a revised report.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

SRAs and their admin staff are security cleared prior to any contract being put in place.

The risks and mitigation described in section 3.1.1 are also relevant.

5.23. Prisoner Location Service

DBS Barring utilise the services of the Prisoner Location Service (PLS) to obtain contact details for referred individuals that are in prison.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

DBS Barring issue requests to the PLS for contact details of referred individuals that are in prison. The request contains the referred individual's nominal details to identify the person. The response confirms the prisoner's location details which can include the prisoner number and prison name or release date details.

Prisoner location requests and responses will be sent through a DBS online account. The DBS online services provide secure methods for communication as described in section 4.1.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

Prisoner location details are required so that correspondence relating to a referral can be sent to a referred individual at the correct address/location. Receiving prisoner location information minimises the risk of referral information being sent to an incorrect address.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Data is retained in accordance with the DBS's DRP as described in section 3.2.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

Security controls for the Home Office network are in place as per HMG Security Framework and security standards to protect against attack.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

Once agreement is made with the PLS from R1, all requests and responses will be made using their DBS online account. The DBS online services provide secure methods for communication as described in section 4.1.

If the PLS does not agree to use a DBS online account, the current process of sending requests and receiving responses by email will be used. The email process also provides a contingency if for any reason the DBS online account cannot be used. This ensures that DBS Barring will be able to continue receiving prisoner location details as they themselves mitigate the risk of correspondence and MTB bundles being sent to incorrect addresses.

f) How could risks associated with individuals being unaware of the collection be mitigated?

No additional risks have been identified.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.24. General Register Office

The General Register Office (GRO) maintains the national archive of all births, marriages and deaths. DBS Barring uses the GRO to confirm deaths.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

If DBS are notified that a referred individual has died, confirmation of the death is needed to ensure the correct data destruction can be undertaken. If an individual dies whilst being considered, there is no need to continue consideration of the referral case.

DBS Barring holds an agreement with the GRO to enable us to request and receive death certificate information.

A DBS Barring casework officer enters the deceased person's nominal details into the GRO website. The GRO then issues a copy of the Death Certificate which contains the person’s details and the date and circumstances of death by post.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

The death certificate is used as evidence to confirm that an individual has died. This information ensures DBS Barring do not continue to process information relating to a deceased individual.

c) What are the risks associated with how long data is retained and how they might be mitigated?

Confirmation of death is needed from the GRO to confirm that the data held in relation to a referred individual is no longer required. The data is dealt with in accordance with the DBS DRP.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

No additional risks have been identified.

f) How could risks associated with individuals being unaware of the collection be mitigated?

No additional risks have been identified.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

5.25. Independent Inquiry into Child Sexual Abuse

The Independent Inquiry into Child Sexual Abuse (IICSA) was set up under the Inquiries Act 2005 by the Home Office on 12 March 2015 in order to investigate whether public bodies and other non-state institutions have taken seriously their duty of care to protect children from sexual abuse in England and Wales.

a) Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

As the IICSA has just begun, it is not yet known if any information gathered by the IICSA will be shared with DBS, and likewise it is unclear how much information IICSA will request from DBS. The Inquiries Act and the IICSA Terms of Reference place wide obligations on all bodies that may hold information with regard to Child Sexual abuse. Currently there are no risks identified, however, this may change as the IICSA evolves.

b) Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

No additional risks have been identified.

c) What are the risks associated with how long data is retained and how they might be mitigated?

No additional risks have been identified.

d) What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

No additional risks have been identified.

e) Given the external sharing, what are the privacy risks and how might they be mitigated?

The IICSA can request information from the DBS. This information could range from corporate facts and figures to specific case information. DBS have set up a central point of contact in DBS for any requests for data from IICSA. This ensures that requests are valid and information is only disclosed after careful consideration by DBS Legal and Information Governance if DBS are permitted to do so. It should be noted that the IICSA has separate physical offices on both DBS sites in Liverpool and Darlington.

f) How could risks associated with individuals being unaware of the collection be mitigated?

Whilst considering a case, the referred individual is notified that the DBS may share information with other parties if required if legislation permits DBS to do so.

g) What are the privacy risks associated with redress and how might they be mitigated?

No additional risks have been identified.

h) Given access and security controls, what privacy risks were identified and how might they be mitigated?

No additional risks have been identified.

6. OVERVIEW

The design and implementation of the R1 Modernisation Solution has greatly mitigated a number of key privacy risks that DBS was facing and some of these risks have been removed completely. Prime examples of this are the introduction of paperless working within Barring and the more rigorous RBACs.

There are a number of items that TCS were unable to deliver in time for R1 go-live and these items will be planned in for a future release date. Therefore, this PIA is a living document and will be reviewed as new functionality is planned to be delivered.

As this PIA covers all of DBS, it will be reviewed regularly to ensure the DBS is continuing to manage and mitigate privacy risks successfully.

DBS will continue to manage all corporate and project relating risks and issues. The risk registers can be found in the relevant folders on the corporate file plan.

7. APPENDIX A - LIST OF DATA ITEMS

List of the Data items DBS collects to enable them to carry out their statutory functions for Disclosure and Barring Services:

- Title
- Surname
- Forename(s)
- DoB
- Place of birth (town)
- Place of birth (country)
- Age
- Previous names / alias names
- Alias DoB
- Gender
- Nationality
- National Insurance Number
- Address inc town/city, country
- Address History
- Dates at address
- Postcode
- Country
- Contact Address
- Home telephone
- Mobile number
- Work telephone number
- Email address
- Professional Regulator
- Registration Number
- Date of Registration
- Teachers Pension Number
- CRB Disclosure number
- Driving licence number
- Passport number
- Scottish vetting & barring number
- Declaration of intention to work paid or unpaid with children, vulnerable adults or both
- Security information name of first school for use when contacting DBS
- Qualifications
- Training History
- In service training
- Role title
- Type of role paid/voluntary
- Date started
- Date ceased
- Reason ceased
- Was the role in regulated activity children/vulnerable adults/both

- Role if still employed
- Role Description
- Whether an individual has lived / worked in Scotland
- Previous misconduct information
- Previous employment
- Reason for referral
- Summary of circumstances
- Other Organisation/Agencies involved
- Chronology of events
- Details of individual put at risk of harm
    - Title
    - Surname
    - Forename
    - DoB
    - Age
    - Gender
    - Relationship to referred person
    - Details of any vulnerability
- Documentation supplied
    - Application for employment
    - References
    - Interview Report
    - CV / Resume
    - Letter of employment offer
    - Job Description
    - File notes
    - Care Plans
    - Victim impact reports/statements
    - Internal investigations and outcomes
    - Documentation of any past disciplinary action/complaints
    - Internal disciplinary action and outcome
    - Statements
    - Investigation and reports of regulatory bodies
    - Investigation and reports of other agencies or bodies
    - Interview report relating to referral
    - Witness statements
    - Dismissal / resignation / redeployment letters
    - Local Authority investigations reports / documents
    - Adult Social Care or Children's Services reports
    - Police investigations and reports
    - Minutes of Strategy meetings
    - Health and Social Care trust Investigations reports / documents
- Referring party details
    - Primary contact details
    - Alternative Contact details

8. APPENDIX B - KOR LIST

List as per SVGA paragraph 41 http://www.legislation.gov.uk/ukpga/2006/47/section/41

Care Council for Wales (CCW)

Education and Training Inspectorate (NI) (ETI)

Education Workforce Council (EWC)

General Chiropractic Council (GCC)

General Dental Council (GDC)

General Medical Council (GMC)

General Optical Council (GOptC)

General Osteopathic Council (GOstC)

General Pharmaceutical Council (GPhC)

General Teaching Council Northern Ireland (GTCNI)

Health and Care Professions Council (HCPC)

Northern Ireland Social Care Council (NISCC)

Nursing and Midwifery Council (NMC)

Pharmaceutical Society of Northern Ireland (PSNI)

9. **APPENDIX C - SA LIST**

As per SVGA paragraph 45 (7) http://www.legislation.gov.uk/ukpga/2006/47/section/45

Care and Social Services Inspectorate Wales (CSSIW)

Care Quality Commission (CQC)

Charity Commission (CC)

Charity Commission for Northern Ireland (CCNI)

Children's Health and Social Services Directorate, Wales (CHSSD)

Education & Training Inspectorate (ETI) Northern Ireland

Estyn (Education and Training Inspectorate for Wales)

Health Inspectorate Wales (HIW)

National College for Teaching and Leadership (NCTL)

Office of the Public Guardian (OPG)

Ofsted

Regulation and Quality Improvement Authority (RQIA)