

Atlantic Data – NHS DBS Service

1. Service Overview

The Atlantic Data - NHS DBS Services provide cloud-based software and managed service capabilities that support organisations in meeting their safeguarding, compliance, and governance obligations relating to Disclosure and Barring Service (DBS) checks.

The services support the full lifecycle of DBS-related safeguarding activities, including DBS application processing, identity and eligibility management, DBS Update Service status checking, and managed safeguarding assurance models designed to maintain ongoing visibility of DBS status over time.

The services are delivered by a specialist DBS provider with extensive experience supporting NHS Trusts and NHS-aligned organisations. The services are used in safeguarding-critical healthcare environments where accuracy, consistency, auditability, proportionality of decision-making, and alignment with NHS governance standards are essential.

This service description applies to the **Atlantic Data – NHS DBS Service**, which is configured specifically for NHS organisations and NHS-aligned environments. The service may operate under either an Umbrella Body model, where Atlantic Data acts as the DBS Registered Body, or a Registered Body model, where the NHS organisation acts as the DBS Registered Body. The selected operating model and service configuration are aligned to NHS governance and assurance requirements.

2. Service Scope

This service description covers the Atlantic Data – NHS DBS Service, which provides DBS checking and safeguarding support configured to meet NHS operational, governance, and assurance requirements.

The service supports NHS organisations that either:

- Operate under an Umbrella Body arrangement, where Atlantic Data acts as the DBS Registered Body; or
- Operate as a DBS Registered Body, where the NHS organisation submits applications directly to the Disclosure and Barring Service.

Included

The Atlantic Data – NHS DBS Service includes:

- Cloud-based DBS application and case management
- Management of DBS application initiation, processing, and tracking
- Identity verification in accordance with DBS requirements and NHS guidance

- Validation and quality checks to support application completeness and accuracy
- Electronic submission of DBS applications to the Disclosure and Barring Service, where applicable
- Management of DBS queries, exceptions, and clarification requests, in line with the selected operating model
- Secure receipt and handling of DBS results
- Management information and audit reporting to support NHS safeguarding oversight and governance

Responsibility for DBS submission and interaction with the Disclosure and Barring Service depends on whether the NHS organisation operates as a DBS Registered Body or under Atlantic Data's Umbrella Body arrangements.

Exclusions

Optional items or services referenced in this document, including those listed at the end (Digital ID, Update Service, Right to Work services), are excluded from the scope of this service unless explicitly stated as included.

3. Customer Journey (End-to-End Workflow)

The NHS DBS Services support a structured end-to-end journey for managing DBS checks and ongoing safeguarding assurance within NHS organisations.

Core DBS Journey

The DBS journey typically follows the stages set out below.

3.1 Service Setup and Configuration

The service is configured in line with the selected Digital Platform item and NHS organisational requirements. This includes organisational structure, user access, role definitions, safeguarding requirements, reporting structures, and the agreed approach to identity verification.

3.2 Application Initiation

A DBS application is initiated by authorised NHS users using the service. Applicants are invited to provide the required information and consent to support the DBS checking process.

3.3 Identity Verification (ID Check)

The applicant's identity is verified in accordance with DBS requirements and NHS guidance. Identity verification may be completed using:

- a manual identity checking process; or

- a digital identity verification process, where this has been selected as part of the service configuration.

Responsibility for completing identity verification depends on the selected operating model and NHS governance arrangements.

3.4 Data Capture and Validation

Applicant information and identity evidence are captured and validated to ensure completeness, accuracy, and eligibility prior to submission. Validation checks are applied to reduce errors and rework during DBS processing.

3.5 DBS Submission

Eligible applications are submitted electronically to the Disclosure and Barring Service via approved DBS submission channels. Submission is performed either by Atlantic Data acting as the DBS Registered Body or by the NHS organisation acting as the DBS Registered Body, depending on the selected operating model.

3.6 DBS Processing and Queries

The Disclosure and Barring Service processes the application. Any queries, exceptions, or clarification requests raised during processing are managed in line with the selected operating model and NHS governance requirements.

3.7 Result Receipt and Reporting

DBS results are received and made available through the service. Management information, audit records, and reporting are updated to support NHS safeguarding oversight and governance.

3.8 Ongoing Safeguarding and Update Service (Where Applicable)

Where the DBS Update Service is included:

- Consent for status checking is managed
- Eligibility for status checks is monitored
- DBS Update Service status checks are performed in line with customer configuration
- Changes, lapses, or loss of eligibility are reported to the NHS organisation

The Update Service operates alongside the DBS application process and does not replace the requirement for a new DBS application where required.

3.9 Safeguarding Oversight

The NHS organisation reviews DBS outcomes and safeguarding information and takes employment or safeguarding decisions in accordance with NHS policies and procedures. The service supports, but does not replace, NHS decision-making responsibilities.

4. Service Features and Capabilities

The NHS DBS Services provide a set of core features that support NHS safeguarding and governance requirements, with additional capabilities enabled depending on the selected operating model and service configuration.

Core DBS Features

The following features are available:

- Cloud-based DBS application and case management
- Secure capture and management of applicant data and consent
- Support for manual and digital identity verification methods in line with DBS requirements
- Validation and quality checks to reduce application errors prior to submission
- Electronic submission of DBS applications via approved DBS channels, where applicable
- Tracking of application status throughout the DBS lifecycle
- Secure receipt and handling of DBS results
- Management information and audit reporting to support NHS safeguarding oversight
- Role-based access controls and segregation of duties
- Configurable workflows to align with NHS safeguarding processes

NHS-Specific Capabilities

Additional capabilities configured for NHS organisations may include:

- Alignment with NHS governance, assurance, and audit requirements
- Portability of Information subject to consent and agreement.
- Support for NHS operational workflows and reporting structures
- Enhanced management information to support NHS oversight

5. Service Delivery Model

The NHS DBS Services are delivered using a combination of cloud-based software and, where applicable, managed service components. The delivery model applied to an NHS organisation is determined by the selected Digital Platform item and operating model.

Cloud-Based Software Delivery

The services are delivered through a secure, cloud-hosted platform accessed via standard web browsers. The platform enables NHS organisations to initiate and manage DBS activity, monitor application progress, and access reporting and audit information.

The software is maintained, updated, and supported by Atlantic Data. Updates and improvements are applied centrally without requiring customer-side installation or maintenance.

Managed Service Components (Where Applicable)

Where the selected service includes managed service elements, Atlantic Data provides operational support alongside the software platform. Managed service components may include:

- Quality assurance of DBS applications prior to submission
- Management of DBS submissions and processing
- Handling of queries and exceptions raised by the Disclosure and Barring Service
- Operational monitoring and issue resolution

Managed services are delivered in accordance with NHS governance expectations and agreed service configurations.

6. Support and Service Management

Support and service management for the Atlantic Data – NHS DBS Service is provided in a structured manner to ensure continuity, reliability, and effective resolution of issues. Support arrangements reflect the safeguarding-critical nature of DBS services within NHS environments.

Support Channels

Support is provided through the following channels:

- Service Desk Support – for day-to-day operational queries, user assistance, and system usage support
- Email Support – for non-urgent requests, reporting queries, and follow-up communication
- Telephone Support – for time-sensitive or safeguarding-related issues

Support channels are available during published support hours. Contact details and access arrangements are provided during onboarding.

Incident Escalation

Incidents and service issues are managed using a defined incident management process. Issues are assessed, prioritised, and progressed based on their impact and urgency.

Escalation routes are in place for:

- Issues affecting DBS processing or result delivery
- Safeguarding-critical incidents

- Service availability or performance concerns

Where appropriate, incidents are escalated internally to specialist teams to ensure timely investigation and resolution.

Service Monitoring and Management

The service is actively monitored to support availability and performance. Atlantic Data maintains oversight of platform operation, managed service activities, and support demand to identify trends and areas for improvement.

Service management activities may include:

- Monitoring of application processing and exception volumes
- Review of support requests and incident trends
- Ongoing service improvement and optimisation

Customer Engagement

NHS organisations are provided with a named point of contact appropriate to the service configuration. Engagement may include onboarding support, service familiarisation, periodic service reviews, and communication of service updates or changes.

7. Service Availability and Performance

The NHS DBS Services are designed to provide reliable and consistent availability to support safeguarding-critical operations within NHS organisations. Availability and performance are managed to ensure services can be accessed when required and that DBS processing activities are not disrupted unnecessarily.

Service Availability

The services are delivered via a cloud-hosted platform that is available to authorised users through standard web browsers.

The platform is designed to support continuous access for operational use, subject to:

- Planned maintenance activities
- Unplanned incidents or external dependencies outside Atlantic Data's control

Where maintenance is planned, NHS organisations are notified in advance where reasonably practicable.

Performance and Reliability

The platform is designed to support the expected volumes and usage patterns of DBS processing and NHS safeguarding oversight. Performance is monitored to ensure that:

- Applications can be initiated, processed, and tracked efficiently

- Reporting and management information remain accessible
- Managed service activities can be carried out without undue delay

Performance management focuses on service stability and operational effectiveness rather than transaction speed alone.

Resilience and Continuity

Measures are in place to support service resilience and continuity, including:

- Redundancy within the hosting environment
- Data backup and recovery processes
- Business continuity and incident response planning

These measures are designed to reduce the risk of service interruption and support timely recovery where incidents occur.

Dependencies and External Services

Certain aspects of the service depend on third-party systems and external bodies, including the Disclosure and Barring Service. Availability and processing times for these external services are outside Atlantic Data's direct control and may affect end-to-end timelines.

8. Security and Compliance

The NHS DBS Services are designed and operated with security, data protection, and regulatory compliance as core principles. Controls are in place to protect personal data, support safeguarding obligations, and meet the expectations of NHS and public sector organisations.

Information Security

Atlantic Data maintains an information security management framework designed to protect the confidentiality, integrity, and availability of service data.

Security controls include:

- Access controls based on defined user roles
- Segregation of environments and duties
- Secure authentication and authorisation mechanisms
- Monitoring and logging of system access and activity
- Regular review and improvement of security controls

Data Protection and Privacy

The services are operated in compliance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Personal data is processed solely for the purposes of delivering DBS and safeguarding services on behalf of NHS organisations. Data handling practices are designed to support:

- Lawful, fair, and transparent processing
- Data minimisation and purpose limitation
- Appropriate retention and secure disposal
- Support for data subject rights

DBS and NHS Compliance

The services are delivered in accordance with Disclosure and Barring Service requirements and guidance, as well as relevant NHS governance and assurance expectations. This includes:

- Adherence to DBS application and identity verification standards
- Secure handling of DBS data and results
- Controls to support auditability and safeguarding oversight

Where Atlantic Data acts as the DBS Registered Body, it is responsible for compliance with DBS operational requirements applicable to that role.

Certifications and Assurance

Atlantic Data holds and maintains relevant certifications and assurance measures to support service security and reliability, including:

- ISO/IEC 27001 certification for information security management
- Regular independent penetration testing conducted by accredited providers
- Compliance with payment security standards where payment processing is applicable

Evidence of certifications and assurance measures can be provided on request.

9. Hosting and Data Residency

The NHS DBS Services are delivered using a secure, cloud-hosted infrastructure designed to support availability, resilience, and compliance with UK data protection and NHS public sector expectations.

Hosting Environment

The services are hosted within a managed cloud environment that supports the secure operation of the software platform and associated managed service components.

The hosting environment is managed and maintained by Atlantic Data and its approved hosting providers. Infrastructure is monitored and maintained to support service availability, security, and performance.

Data Residency

Personal data processed as part of the NHS DBS Services is hosted within the United Kingdom.

Data residency arrangements are designed to support compliance with UK data protection legislation and NHS data governance requirements.

Access and Connectivity

The service is accessed via the public internet using secure connections. Access is restricted to authorised users through authentication and role-based controls.

Backup and Recovery

Backup and recovery processes are in place to support data integrity and service continuity. Backups are managed in line with defined retention and recovery procedures and are tested periodically.

10. Data Management and Retention

The NHS DBS Services manage personal and operational data in a controlled and transparent manner to support DBS processing, NHS safeguarding oversight, and compliance with legal and regulatory obligations.

Data Categories

The services may process the following categories of data:

- Applicant personal information required for DBS applications
- Identity verification information and supporting evidence
- DBS application status and outcome data
- Consent records and audit information
- Service usage, reporting, and management information

Data processed is limited to what is necessary to deliver the selected service and support safeguarding and governance requirements.

Data Processing Roles

Atlantic Data acts as a data processor on behalf of NHS organisations for the purposes of delivering the NHS DBS Services. NHS organisations act as data controllers and determine the lawful basis and purposes for processing personal data.

Data Retention

Personal data is retained in accordance with:

- Applicable legal and regulatory requirements
- DBS guidance and audit obligations
- NHS retention policies and customer-defined retention periods, where permitted

Retention periods and data handling arrangements are agreed during service onboarding and may be reviewed periodically. Data that is no longer required is securely deleted or anonymised in line with defined procedures.

Data Access and Control

Access to personal data is restricted to authorised users and personnel based on defined roles and responsibilities. Controls are in place to prevent unauthorised access, alteration, or disclosure of data.

Data Subject Rights

The services support NHS organisations in meeting their obligations in relation to data subject rights, including access, rectification, and erasure, in line with applicable data protection legislation.

11. Onboarding and Implementation

Onboarding Approach

Onboarding typically includes:

- Confirmation of the selected Digital Platform item and operating model
- Set-up of NHS organisational details, user roles, and access controls
- Configuration of workflows, safeguarding requirements, and reporting
- Agreement of identity verification methods and operational processes

The onboarding process is managed collaboratively to ensure clarity of roles and responsibilities.

Implementation Activities

Implementation activities may include:

- System configuration and environment setup
- User account creation and role assignment
- Data or configuration migration where applicable
- Testing of workflows and reporting

The scope and duration of implementation activities depend on the selected service and organisational complexity.

User Enablement

Users are supported during onboarding through:

- Guidance on system use and DBS processes
- Access to user documentation and supporting materials
- Initial support to ensure users can operate the service effectively

User enablement is designed to support consistent and compliant use of the service.

Go-Live and Early Support

Following onboarding, the service moves into live operation. Additional support may be provided during the early stages of use to address queries, confirm correct configuration, and support a smooth transition into business-as-usual operation.

12. Offboarding and Exit Planning

Offboarding from the NHS DBS Services is managed in a controlled and transparent manner to support continuity, data protection, and safeguarding obligations for NHS organisations. Offboarding arrangements are designed to minimise disruption and support an orderly transition at the end of service use.

Offboarding Approach

Offboarding is initiated in line with contractual arrangements and agreed timelines. The approach is proportionate to the selected service configuration and the nature of the NHS organisation's DBS activity.

Offboarding activities may include:

- Confirmation of offboarding scope and timetable
- Controlled closure of user access
- Agreement of data handling and transfer requirements
- Coordination of any required transition support

Data Handling on Exit

On exit, personal and operational data is handled in accordance with:

- Applicable data protection legislation
- DBS audit and record-keeping requirements

- NHS data retention and disposal guidance

Data may be:

- Returned to the NHS organisation in an agreed format
- Retained where legally required
- Securely deleted or anonymised in line with defined procedures

A record of data handling actions may be provided to support audit and governance requirements.

Continuity and Safeguarding Considerations

Where offboarding occurs while DBS activity is in progress, reasonable steps are taken to ensure continuity and avoid unnecessary safeguarding risk. This may include completion of in-flight applications or agreement of handover arrangements, subject to contractual terms.

13. Customer Responsibilities

NHS organisations using the NHS DBS Services have defined responsibilities to ensure the services are used appropriately, lawfully, and in line with NHS safeguarding requirements.

Organisational Responsibilities

NHS organisations are responsible for:

- Defining roles, eligibility, and safeguarding requirements for DBS checks
- Ensuring DBS checks are requested only where lawful and appropriate
- Maintaining accurate organisational and user information within the service
- Ensuring users are authorised and trained to use the service appropriately

Applicant Engagement and Information

NHS organisations are responsible for:

- Engaging applicants and providing clear instructions
- Ensuring information submitted by applicants is accurate and complete
- Obtaining and maintaining appropriate consent for DBS processing and, where applicable, Update Service status checking

Safeguarding and Decision-Making

NHS organisations remain responsible for:

- Reviewing DBS outcomes and safeguarding information

- Making employment or safeguarding decisions in accordance with NHS policies and procedures

The services support safeguarding decisions but do not replace NHS responsibility or judgement.

Compliance Responsibilities

NHS organisations are responsible for complying with applicable laws, guidance, and NHS policies relevant to their use of DBS services, including data protection and safeguarding obligations.

14. Optional Modules

The Atlantic Update Service

The DBS Update Service may be included as an optional module alongside this service, where the customer has also selected the separate G-Cloud service titled **“The Atlantic Update Service”**. When configured, this module enables ongoing status checking of eligible DBS certificates using the Disclosure and Barring Service Update Service, subject to individual consent and eligibility requirements. The module supports NHS organisations in maintaining ongoing safeguarding oversight by identifying changes to DBS status over time, without removing the need for a new DBS application where required. The scope and operation of the DBS Update Service are defined by the Atlantic Update Service G-Cloud listing and the agreed service configuration.

Digital Identity Service

A Digital Identity capability may be included as an optional module alongside this service, where the customer has also selected the separate G-Cloud service titled **“Atlantic Data Digital Identity Services”**. When configured, this module supports the verification and controlled reuse of digital identity evidence in line with UK government standards, subject to individual consent and applicable eligibility requirements. For NHS organisations, this can support more efficient identity verification processes and reduce unnecessary repeat identity checks, while maintaining appropriate safeguarding, governance, and audit controls. The scope and operation of digital identity functionality are defined by the Atlantic Data Digital Identity Services G-Cloud listing and the agreed service configuration.

Right to Work Service

A Right to Work checking capability may be included as an optional module alongside this service, where the customer has also selected the separate G-Cloud service titled **“Right to Work Services”**. When configured, this module supports the verification of an individual’s right

to work in the UK in accordance with Home Office requirements, using appropriate checking methods based on nationality and eligibility. For NHS organisations, this can support compliant workforce onboarding and assurance processes, while maintaining appropriate governance, auditability, and separation from DBS decision-making. The scope and operation of Right to Work functionality are defined by the Right to Work Services G-Cloud listing and the agreed service configuration.