

Part 2: Specification

Contract Reference: RBGKEW1000

DBS Screening Services

(This document is for information)

1. **Summary**

The aim of this procurement activity is to procure a supplier for the provision of online DBS Screening Services (Standard and Enhanced) for RBG Kew employees and volunteers, commencing in April 2022.

1. **Background**

Royal Botanic Gardens, Kew (‘RBG Kew’) is a world-famous centre for botanical and mycological knowledge. With our two inspiring gardens at Kew in west London and Wakehurst in Sussex, we enchant our visitors with the wonder of plant diversity.

As a visitor attraction with 2.5 million visitors each year, Kew takes its responsibilities for safeguarding seriously.

Kew operates the Baseline Personnel Security Standard (BPSS) for our employees, and all employees are therefore required to obtain a Basic DBS check prior to appointment.

In addition, many of Kew’s public programmes involve engaging with children under 18 and vulnerable adults, and as such those employees and volunteers carrying out regulated activity require an Enhanced DBS check. RBG Kew is increasing its engagement activities with all levels of the community, including a number of family events and volunteering programmes for young people. We also operate a schools learning programme at both Kew and Wakehurst which employs teachers.

There are currently approximately 200 employee roles at Kew which require an Enhanced DBS and approximately 160 volunteer roles. In addition there are a small number of roles which require a Standard DBS. Standard and Enhanced DBS checks are renewed every three years.

Kew uses the services of a third party provider to process Standard and Enhanced DBS checks. The contract with our current provider ends 31 March 2022 and we are therefore undertaking a procurement process to appoint a provider to undertake these services from 1 April 2022.

1. **Scope of the requirements**

The successful Supplier will provide a professional and efficient DBS application processing service to RBG Kew to enable us to complete the following checks on candidates, employees, contractors and volunteers:

1. Standard
2. Enhanced
3. Enhanced with Adult and /or Child Barred Lists

Our requirements from the successful Supplier will be:

1. **Functional Requirements**

**Essential:**

1. A secure online portal for processing of checks with a user-friendly interface, compatible with all major browsers including MS Edge.
2. Clear, step by step instructions for applicants
3. The ability to have separate logins for employee / volunteer checks to be requested.
4. The ability for designated individuals in HR to have overall visibility of all checks submitted.
5. The ability for HR users to track the status and progress of individual applications.
6. Weekly real-time reports showing status of live checks.
7. Email alerts / reminders directly from the provider to inform applicants and HR of outstanding actions as required.
8. Email alerts to HR and applicants when certificates are received. This must include a specific alert where there is content on the certificate requiring review by HR, instructing the applicant to produce their certificate within a specified timeframe.
9. Where required, provision of expert advice to assist with resolution of DBS eligibility queries for individual roles

**Desirable:**

1. Functionality for self-service reporting for HR users with the ability to export reports to Excel if needed.
2. Ability to view DBS check history within the system and report on this.
3. Provisions for update service management within the service and system
4. **Customer Service & Support**

**Essential:**

1. Effective dissemination of important information e.g. acceptable documents for DBS checks and any changes in legislation or policy
2. Proactive communication regarding issues e.g. problem with an individual check, or with the service / system e.g system downtime.
3. A responsive customer support service which includes the ability to contact the provider via a designated helpline and email address immediately should Kew or applicants have any queries or problems. As a minimum this must be available during standard business hours i.e. 9am to 5pm, Monday to Friday
4. Wherever possible, communication to resolve issues with individual applications should be conducted directly with the applicant to avoid unnecessary delays, whilst ensuring Kew is kept fully informed.
5. Designated named point of contact within the screening / operations team for day to day queries.
6. Designated account manager able to facilitate resolution of any service issues.

**Desirable:**

1. Live chat option via portal
2. **Performance Requirements**

On average, Kew processes approximately 94 checks per annum on average for employees (majority Enhanced with Child Barred List) and 30 for volunteers every year. A breakdown of volumes over the previous three years for employee checks is provided below for reference. the service must be capable of handling this volume and dealing with periodic peaks in usage e.g. for seasonal intakes of workers / volunteers or large batches of renewals.

|  |  |
| --- | --- |
| **Time Period** | **No of employee checks** |
| 1/10/20 - 30/09/21 | 127 |
| 01/10/19 - 30/09/20 | 65 |
| 01/10/18 - 30/09/19 | 90 |

The provider must have relevant KPI’s in place and robust systems for measuring and monitoring performance against these, as a minimum this must include;

* processing times I.e. time from application being requested through to submission to Disclosure and Barring Service, and time from receipt of certificate to notifying client of result.
* call / email handling, I.e. timeframes for responding to email and phone enquiries from clients and applicants.
* timeframes for resolution of applicant / client problems or issues
* The provider must be able to demonstrate responsive, pro-active and effective troubleshooting in relation to any blockers or problems in the application process e.g. where unsatisfactory documents are provided.

The provider must be able to demonstrate a good level of customer satisfaction from other clients and be able to evidence this e.g. via testimonials or customer satisfaction scores.

1. **Implementation**

The provider must be able to demonstrate a comprehensive implementation plan to ensure minimal service interruption and a smooth transition from the previous contract.

The service must be fully operational by 1 April 2022.

Implementation must include system training for HR and other admin users , along with provision of comprehensive user guides etc.

1. **Contract governance**

Kew will require quarterly MI reports with information relating to checks processed, performance against agreed KPI’s etc.

Account reviews with designated account manager will take place at least quarterly in the first year of the contract and thereafter at least annually.

Account review meetings will include;

* Review of MI and performance
* Business updates including legislative or process changes
* Discussion and resolution of any operational or service issues

1. **Data Protection**

The provider will be expected to support Kew with its data protection obligations under the UK General Data Protection Regulation and the UK Data Protection Act. This includes, but is not limited to, data protection contractual clauses, data protection impact assessments and further data protection due diligence.

It is preferred that the provider be established in the UK and that personal data be hosted in the UK. If the provider is established overseas or data will be hosted overseas, the provider must specify the data transfer mechanism and how sensitive personal data will be safeguarded when transferred.

The provider will be expected to inform Kew of any personal data breaches and of any enforcement action taken against you by a data protection regulator in the last three years.

The provider will be expected to share with Kew the outcomes of any personal data and/or security audits that have taken place in the last three years.

The provider should clarify its role in the personal data processing. In particular, the provider should specify whether they will be a data controller or a data processor for all or part of the personal data processing.

1. **IT security requirements**

|  |  |
| --- | --- |
| **Essential** | **Desirable** |
| Suppliers offering cloud/hosted solutions must be certified to ISO27017 and ISO27018 compliant. Or Equivalent. | Suppliers are ISO9001 compliant to support quality evaluation. Or Equivalent |
| Supplier must describe and provides evidence of, its approach to incident reporting and problem management. |  |
| The system provides a secure browsing experience using a HTTPS public trusted certificate to encryption standard TLS1.2 minimum. |  |
| All data in transit must be encrypted. |  |
| All data at rest must be encrypted. |  |
| The system provides assurance on the integrity of its electronic records and associated raw data by logging all the functions performed by users as well as system generated actions. To ensure the integrity of the logs, each log should be dated and timed to establish the sequence of events as well as to record the account (user or service) that generated the log(s). Items to be recorded include: (1) User action (view, create, edit, delete) (2) System action (view, create, edit, delete) |  |
| The system must incorporate full backup and restore facilities and audit trails. |  |
| The system provides support for all password rules and complexities defined by the organisation (Complex Passwords). | The function granting user permissions and authentication for the System is capable of being fully integrated with Microsoft Azure AD. |
| The system provides secondary means of authentication using a two factor/multi-factor mechanism. This will be dependent on risk and at a minimum apply to administrative accounts of the system. |  |
| The system supports role-based security features where appropriate (Role Based Access Control (RBAC)). |  |
| The system must be accessible and operational at least 99.9% of the time during any 3-month period (the “Availability”). The Availability excludes any agreed downtime for maintenance, which should not exceed 4 hours in any 3-month period |  |
| The Supplier must provide changes to software required by legislation at no additional cost to the organisation. |  |
| Any upgrades or enhancements to the system are included in the cost of the maintenance contract for the System. |  |

1. **Other standards**

Suppliers must be compliant with the Revised Code of Practise for DBS Registered Persons and associated relevant legislation including Rehabilitation of Offenders Act 1974.

1. **Payment profile**

Invoices to be emailed to [hr@kew.org](mailto:hr@kew.org) monthly and include an itemised statement.

1. **Contract Terms**

Suppliers will be expected to contract with Kew under its standard service terms (included in this ITT). We will not accept any amendments to be made to the legal terms but do expect to adapt the data processing section in Part 1 and the related Schedule to reflect the business model if needed, such as where you may be processing as a data controller, rather than data processor.