Request for information

Barred and Advisory List

Response deadline: 28/03/2022 12 Noon

Table of Contents

Introduction 3

The College of Policing 4

Background 5

Desired Outcomes 6

The requirements 7

Outline of requirements 8

System Users 8

System Functionality 9

Management information 11

Usability, compatibility and accessibility 11

Technology, security and hosting 12

Incident management, support and maintenance 12

Product and service management 13

Future improvements 13

Request for Information Questionnaire 14

# Introduction

The College is conducting early market engagement in the form of this Request for Information (RFI) in order to explore potential solutions that could meet its requirements as set out in this document.

Contained within this document is a background to the project and the requirements along a series of questions that we seek responses to from interested parties.

The responses to this document will be used to inform an Outline Business case for the project and help inform the future direction we take both in terms of the solution and any future procurement process.

By responding to this RFI, should your responses be of interest to the College we may in the future seek further engagement with you in order to better inform our approach to any future procurement.

# The College of Policing

The College of Policing (the “College”) is the Professional Body for all in policing in England and Wales. ​Working together with everyone in policing, we share the skills and knowledge officers and staff need to prevent crime and keep people safe.

We set the standards in policing to build and preserve public trust and we help those in policing develop the expertise needed to meet the demands of today and prepare for the challenges of the future.

We have a mandate to set standards in professional development, including codes of practice and regulations, to ensure consistency across the 43 Home Office (HO) forces in England and Wales.

We also have a remit to set standards for the police service on training, development, skills and qualifications, and we will provide maximum support to help the service implement these standards.

Further information is available on the College website: [Working together | College of Policing](https://www.college.police.uk/)

The College has 4 locations:

* Spring Gardens, London
* Ryton-on-Dunsmore near Coventry
* Harperley Hall, Crook, Co. Durham
* Harrogate

# Background

National Barred and Advisory Lists project is looking to procure a new case management system to better record, share and retain information relating to the Barred and Advisory lists held by the College. The barred list contains details of all officers, special constables and staff members who have been dismissed from policing after investigations under the Police (Conduct) Regulations 2012 or Police (Performance) Regulations 2012 as well as the equivalents for police staff.

The police advisory list is a list of all officers, special constables and staff members who have resigned or retired during an investigation or who leave before an allegation comes to light. It also includes designated volunteers who have had their designated status withdrawn because of conduct or performance matters. More information on the barred and advisory lists can be found on the following webpage - [Barred list | College of Policing](https://www.college.police.uk/ethics/barred-list)

Both the Barred and Advisory lists are used to inform the recruitment and vetting process for 43 HO territorial forces and provide access to the lists to other non-HO forces and agencies via Information Sharing agreements (ISA), to determine if an individual is suitable to be employed. The aim is to have a central store for both lists which can route out the public facing content to the College website and enable a secure means for vetting officers to access other content.

In order to manage the information relating to the Barred and Advisory lists the College must find a solution that is secure, easily updated, can store all information relevant to each record and provide access to all users across Forces and the College. Users are allocated a user level when they are invited to join the system which will only allow them to see information relevant to their role and prevent changes to records being made by someone without correct authority.

The basic function of the system should allow police force inputters to submit details of officers and staff who have either been dismissed or have resigned or retired whilst under investigation. Access will be via an online portal system using multi factor authentication, and the system must be able to record all information and decision making under individual records created for each person.

The College of Policing will check the information for accuracy, and will either agree and provide a system generated reference number to the force, or ask the force to provide more information prior to agreeing the information they have sent. If somebody has been dismissed they will be entered onto the barred list. If somebody has retired or resigned whilst under investigation they will be placed onto the advisory list. The information required to be submitted by police forces is exactly the same for both lists.

The College is also responsible for the Review Process which under Legislation allows individuals to apply for removal of their barred status after a period of time following dismissal. The College makes the final determination after looking into details of a case, and an individual’s barred status is only removed where the College deems it appropriate~~.~~

In summary, the College is seeking to find a solution which provides more automation, better accessibility, better security, less margin for error, and mitigating the potential for information breaches.

# Desired Outcomes

A new holistic solution should allow us to manage data relationships, documents, and processes in a single product, empowering employees to effectively manage individual cases and make better business decisions. We would expect to see the following:

* **Increase productivity and ensure continuity with a complete view of information.** Rather than having to toggle between systems or manage spreadsheets, staff remain within the same intuitive interface, logging activities, adding notes and updates, delegating tasks, and scheduling events.
* **Improve visibility and control.** Reporting dashboards and audit trails of all activities increase transparency, support compliance and help organisations identify opportunities for improvement.
* **Ensure smooth handoffs and effective collaboration.** With critical information and supporting content instantly accessible to all authorised employees, organisations support effective collaboration.

Envisaged benefits to the College:

* More effective risk controls on data security and integrity
	+ Reduced vulnerability to unwitting use of inaccurate data
	+ Reduced vulnerability to regulatory sanctions for non-compliance
	+ Reduced reputational risk
	+ Integrity, Ethics and Professional standards met
* Improve experience for College and Force users and members of the public
	+ Trusted source of B&A Information
	+ Effective information handling processes
	+ Public register only shows relevant results based on search not full list
* Improved productivity for data administration tasks
	+ Improved productivity of administration teams
	+ Centralised records maintenance and workflows
	+ Comprehensive case histories including key decisions
	+ Automatic alerts and prompts can be created
	+ Automatic publication of relevant information
	+ Automatic removal of time-expired records from public viewing list
	+ Audit trails secured against each record
	+ Security and access rights set up for each user
	+ Management and statistical reporting can be produced
	+ FoI and Subject access requests can resolved much quicker

# The requirements

We are seeking to replace the current system with a more modern solution that provides greater flexibility and a better user experience going forward. Any future solution must have the ability to integrate with our College website. In the future we will expect suppliers to work with us to integrate with Forces system such as Centurion which is widely used by forces currently. By way of example the barred list can be searched via our website at the following address - [Search the barred list | College of Policing](https://www.college.police.uk/ethics/barred-list/search-the-barred-list)

The need for these changes has been driven by customer feedback and a need to significantly improve the now outdated design of the current system. The new platform will need to ensure the system can be customised and aligned to the College branding so that it is more in-keeping with other College systems like the [College website](https://www.college.police.uk/) and [College Learn platform](https://www.learn.college.police.uk/Account/Landing). The platform will also need to meet necessary accessibility and security requirements.

The platform will be used by HO Forces to submit details of individuals who are required to be listed on the Barred and Advisory lists and support this being done securely and in-line with our legislative requirements (i.e., in line with, Police (Conduct) Regulations 2012 and Police (Performance) Regulations 2012)

The platform will host two lists (Barred and Advisory), however, the management of the records within the system will take all take place within one system. The barred list will need be made available to be searchable by the public using an API. This is currently done through the College website as per the link provided earlier in the document.

# Outline of requirements

We have identified a series of features and functionality we would like the new platform to have:

## System Users

**Barred List**

* Ability to set user access levels based on role within College and Force
* Allow users access to Barred List depending on security level
* Allow public users to search Barred list using:
	+ First name
	+ Last name
	+ Alias
* Allow vetting staff from forces and agencies to search Barred list using:
	+ First name
	+ Last name
	+ Alias names
	+ Date of Birth
	+ Collar number
	+ Force PSD reference number
	+ Details of person who submitted e.g., name, email address
* Restricted access to biodata to the College only except for the force that uploaded the record
* Allow public user to access search Barred list through College website
* Restrict shown entries to those based on search criteria

**Advisory List**

* Ability to set user access levels based on role within College and Force
* Force users can only access records added by their force except for in the cases of forces that share information and administration
* Allow users access to Advisory List depending on security level
* Allow vetting agents to search any record on the Advisory list using:
	+ First name
	+ Last name
	+ Alias names
	+ Date of Birth
	+ Collar number
	+ Force PSD reference number
	+ Details of person who submitted e.g., name, email address
* Restricted access to protected characteristics to the college only
* Restrict shown entries to those based on search criteria

**User Access**

* Allow College and Force users to login to system – multi factor authentication
* Requirement for new users to agree to Terms of Use and Privacy Notice
* Ability to set access levels for all user roles and groups – Super users from College Admin only
	+ Access levels to be set:
		- Level 1 – Ability for the public to search records
		- Level 2 – Force basic administration rights to input and view own force records.
		- Level 3 – For vetting reasons - Ability for Force/Agency vetting staff to search any record on the Barred or Advisory List
		- Level 4 – College of Policing Super user administration rights to change, approve, amend, publish and transfer information from Advisory to Barred lists – Force and College
		- Level 5 – College of Policing General systems administration rights
* Ability to create new users – Super users from the College only
* Ability to configure new workflows within the College as necessary – Super users from College Admin only
* Password resets to be done by Forces Administrators – Super Users only
* Ability to publish records to public list – Super users College Admin only
* Ability to restrict access on any record where necessary – Super users College Admin only

## System Functionality

* Flag automatically set up on case as an alert to College Admin 11 months after creation to remove sensitive data by College Admin
* Records to be created using drop down data choices whenever possible
* Requirement to add details against each record
* Ability to upload additional documents to each record
* Ability to assign record to specific person(s) for action with full audit trail
* Ability to link records
* Any links to other records to be shown clearly on record and can be accessed through each other
* Any records that are no longer live remain linked for reference but can be redacted when closed
* Ability to record in audit trail who submitted/created the record
* Ability to contact people in audit trail by clicking on name within record to bring up contact details such as phone and email
* Ability to record date of any appeals within record
* Ability to choose if appeal successful/ not successful
* Ability to choose person responsible for decision
* Ability to record date of appeal
* Ability to record date of decision
* Ability to record appeal information
* Ability to record full audit trail for appeal information
* Ability to record publication decision
* Ability to record full audit trail for publication decision
* Ability to complete a risk assessment form to request records are exempted
* Ability to return results based on misspelling or different name spellings e.g. Steven/Stephen
* Only show entries based on search criteria
* Ability to flag duplicate records when system recognises existing data being entered into same fields
	+ Option to choose and update existing record
	+ Option to continue creating new record with same information
	+ Option to link two or more records together
* Ability to manage reminders and alerts for review dates and removal of sensitive data
* Forces Inputters to access online submission form
* Ability for system to automatically create record from online form sent to secure mailbox
* Generate reference number to send back to force inputter for future reference
* Ability to automatically reject records from being created if form not correctly completed e.g., missing data in mandatory fields
* Ability to put records into ‘draft/incomplete’ status while additional information is gathered but still be visible to searches from users with correct access level
* Automatically adds to Barred or Advisory or draft/incomplete’ list based on information submitted on online form
* Functionality for templates within inputting form
* Functionality to categorise standards of professional behaviour breached and associated behaviours (violence, sexual etc).
* College Super User can manually change status of record from draft to Advisory to Barred and all additional information will update automatically e.g. flags for removal date etc.
* Ability to lock fields so that only those with permission can change them
* Mandatory audit trail showing:
	+ Date of Change
	+ Name of person making the change
	+ Reason for the change
* Ability to assign actions to the record inputter to change or update records
* Flag fields that need action with colour in record

## Management information

**Management Information and Reporting**

* High level report to show how many new entries created each month for each list
* Ability to generate statistical data that can:
	+ Provide dismissal data for Police Officers, Special Constabulary and Police Staff for each force
	+ Dismissal whilst serving, resigned or retired
	+ Total monthly and annual dismissals
	+ Dismissals by Rank
	+ Identify which Standards of Professional Behaviour have been breached
	+ Identify Categories of Dismissal
	+ Provide Protected Characteristic breakdowns
	+ Calculate officers exempted from the public list
* Variety of configurable reports can be generated based on force, date, etc
* Data analysis option to report on Protected Characteristics/ biodata
* Report to show entries that are flagged each month as needing change e.g. removal of list
* Ability to store and run reports over 12 months for comparison
* Ability to export data into excel/csv files

## Usability, compatibility and accessibility

* The platform must be capable of running on any device, operating system and browser from IE11 upwards or equivalent.
* Customisable to reflect College branding
* Administrators can be assigned different access rights to the platform dependent on their level of access
* Good user experience – system should be clear and easy to use for users
* Platform should be tested and work with the following assistive technologies across Chrome, Firefox, Safari and MS Edge browsers (where applicable),
	+ JAWS (desktop screen reader)
	+ NVDA (desktop screen reader)
	+ Dragon (speech recognition)
	+ Windows Magnifier or Apple Zoom (screen magnifiers)
	+ VoiceOver (iOS only) (mobile screen reader)
	+ TalkBack (mobile screen reader)
* Compatible with assistive software
* An option to have the ability to use the Welsh language
* Would be required to meet the [Web Content Accessibility Guidelines (WCAG) 2.1 (w3.org)](https://www.w3.org/TR/WCAG21/) design principles prior to any User Acceptance Testing
* Accessibility statement which confirms platform meets the WCAG 2.1AA requirements. Here is a link to a [sample accessibility statement](https://www.gov.uk/government/publications/sample-accessibility-statement/sample-accessibility-statement-for-a-fictional-public-sector-website) (for a fictional public sector website) - GOV.UK (www.gov.uk) to show what is required

## Technology, security and hosting

* This system is going to be handling OFFICIAL SENSITIVE data
* Uses Multi-Factor Authentication (MFA) as for administration users in line with government guidance
* Meets following security assurance standards:
	+ Cyber Essential plus and/or ISO27001 and/ or SOC2/3 accreditation
* The supplier must agree to work towards the following over the life of the agreement:
	+ NPIRMT Candidate Control Set for Suppliers
	+ OWASP Testing
* Meets all requirements under UK data protection legislation (GDPR, DPA 2018) and the standards required by the College including wider information law compliance such as freedom of information and transparency
* Data stored/platform hosted in UK or European Economic Area
* CHECK Green Light ITHC completed annually on platform, or permission for the College to do this (may include testing the hosting environment). All findings must be made available to the College with a summary of what hasn’t been fixed
* There is an audit of data access, amendment, deletion and export
* System is stable and there are fall back and recovery processes in place
* System protects authentication information against misuse or compromise
* Data is securely held and managed in line with protocols
* All staff who have access to the system vetted at. NPPV2 for non-privileged users and NPPV3 for privileged users
* Solution complies with NCSC14 Cloud Security Principles

## Incident management, support and maintenance

* Documented life cycle management processes for the platform must be in place
* Qualified supplier resources identified to support the platform alongside the College
* Prompt resolution of incident and service requests
* Database of fixes and known errors
* Clearly defined process for managing incidents and problems
* Clearly defined maintenance process
* Comprehensive fall back and recovery processes are in place to reduce disruption to the system

## Product and service management

* Supplier to perform application and platform management of the system in line with contractual obligations
* Supplier to provide tools for defect logging and project communications
* Supplier to provide critical applications support
* Supplier meets our agreed resolution times for incidents and problems
* Supplier signs up to our Service Management Agreement
* Supplier provides College with access to system back-ups
* Supplier to provide, configure, deploy and manage the cloud hosting platform
* Supplier to monitor hosting
* Supplier to have a disaster recovery plan in place
* Supplier to ensure appropriately qualified staff are available for service management

## Future improvements

* Ensure platform is flexible enough to change in order to meet future requirements to ensure the College can keep up with other commercial systems that are available in the marketplace

# Request for Information Questionnaire

Please provide answers to the following questions and return your response to the following email address by the response deadline on the front cover of this document

CPU.Tenders@college.police.uk

|  |
| --- |
| **Response – General Questions** |
| Please provide a brief introduction to your company: |
|  |
| Please provide the name of the solution you offer: |
|  |
| Is this your solution or do you provide a third party solution? |
|  |
| What would a typical timeframe be for the implementation of your solution and what would the project phases look like? |
|  |
| What would be the cost of implementing your solution? (please include one off/annual licensing/per user costs based on approximately 750 users annually) |
|  |
| Can you provide any references or case studies evidencing the use of your solution? (please provide links or documents if possible) |
|  |
| Further to the functionality requirements we have detailed in this document are there any other features or functionality that we have not listed that you believe may be of value to the College? (please provide an overview of why these features or functionality should be built into our final specification) |
|  |
| Please provide any feedback on the specification we have provided: |
|  |
| Does your organisation sit on any Public Sector Frameworks that would be accessible to the College and would be suitable for Procuring this type of requirement? If so please can you provide the detail of the Framework below. |
|  |
| Using the table below please identify if the system you offer provides the required functionality. Please also provide further information about how your proposed solution meets this requirement. |
| **System Users** | **Does your solution provide this functionality?** |
|  |
| **System Functionality** | **Does your solution provide this functionality?** |
|  |  |
| **Management Information** | **Does your solution provide this functionality?** |
|  |  |
| **Usability, compatibility and accessibility** | **Does your solution provide this functionality?** |
|  |  |
| **Technology, security and hosting** | **Does your solution provide this functionality?** |
|  |  |
| **Incident management, support and maintenance** | **Does your solution provide this functionality?** |
|  |  |
| **Product and service management** | **Does your solution provide this functionality?** |
|  |  |
| **Future improvements** | **Does your solution provide this functionality?** |
|  |  |