SECTION B

SCHEDULES

SECTION B.1

SCHEDULE 1 – Statement of Requirements/Specification for a User Journey, Citizen Portal, and Customer Relationship Management solution

to

Bedfordshire Police, Cambridgeshire Constabulary, Hertfordshire Constabulary, Norfolk Constabulary, Suffolk Constabulary, Kent Police and Essex Police

Contents

1. Glossary

Contact Management	The first point of contact into policing and the criminal justice system.
Contact Management Colleague	Police Staff/Officer that takes the initial action to determine the required response and level of risk to the public following contact from the public.
Crime	An incident recorded by the police, assessed as potentially criminal and resulting in the necessity for further investigation.
Digital Asset Management System (DAMs)	Application for storing and receiving digital content, including body worn footage and CCTV/Media files.
Digital Public Contact (DPC)	A programme commissioned by the National Police Chief's Council (NPCC) that aims to improve how the public can contact the police digitally.
Eastern Region	Bedfordshire, Cambridgeshire, Hertfordshire, Kent, Essex, Norfolk, and Suffolk police forces.
Failure Demand	Members contacting to request an update on their report or to speak to their Investigating Officer.
Functional Requirements	The user/business functionality requirements to be met by the solution(s).
Incident	An occurrence identified by or reported to the police which has been assessed for potential deployment.
National MyPolice Portal (NMPP)	A nationally consistent service providing a range of interactive digital services including status updates, two-way communications, and community engagement.
Non-Crime	An incident recorded by the police, but after being assessed for potential deployment, has been deemed as not involving any criminal actions.
Member of Public (MoP)	Member of the Public includes Reporters (victims, witnesses, reporters on behalf of), Applicants, Requestors and Complainants. A registered MoP can take on several roles and can be Individuals, Nominees to manage account 'for others' or associated with an Organisation.
PEEL Inspection	PEEL (police effectiveness, efficiency, and legitimacy) are the regular assessments conducted by HMICFRS of police forces in England and Wales to assess how good forces are in several areas of policing.
Police Information and Records Management (PIRM) 2023	The replacement code for Management of Policing Information (MoPI) 2005 and is a broader standard code which governs the way in which all police information and material is managed and handled by Forces.
Single Online Home (SOH)	National web-based platform providing digital reporting services for 43 police forces across England and Wales, and the British Transport Police. It aspires to be a digital front counter for the public, offering a broad range of online police services.
Victims Code of Practice (VCoP)	The services and a minimum standard for the services that must be provided to victims of crime in England and Wales. The Rights that apply to individuals depend on whether the crime is reported to police, if the case goes to court, whether the defendant is convicted, as well as personal needs/circumstances.

Web Content Accessibility Guidelines	An internationally recognised set of recommendations for improving web accessibility, explaining how to make digital services, websites, and apps accessible to everyone.

2. Background and Objectives

2.1. With Contact Management typically the first point of contact for the public when contacting Police, it is important that there is a consistent and well performing service that meets the demand accurately and appropriately, through public channels of preference, whether that be telephony or digital.

2.2. Police Contact Management demand is continually increasing, partly due to the quantity of failure demand, abandoned calls and public using the 999 and 101 services instead of other available channels. As a result, dissatisfied victims often cite having to chase Police for updates, not receiving updates or having to wait for an Officer. Contact Management demand issues are further compounded by the lack of integration which requires a Contact Management colleague to manually search multiple systems for information whilst on a call with a member of the public and double key information across multiple systems.

2.3. Police forces across the Eastern Region are therefore keen to invest in technological solutions that can meet individual force needs and achieve the following objective(s):

- Improve experience of members of the public accessing the policing service,
- Provide the public with consistent updates in a timely manner,
- Improve public trust, confidence, and satisfaction,
- Reduce Contact Management demand,
- Improve force's overall Contact Management performance.

2.4. To achieve these objectives and support benefits realisation, three key aspects of technological functionality have been identified in relation to victim self-service and customer relationship management: User Journey, Citizen Portal, and a Customer Relationship Management tool.

2.5. **(1) Victim Self-Service**

2.5.1. Victim Self-Service Current State

In addition to traditional methods of contacting police (999, 101, enquiry offices, and social media), forces currently use the national Single Online Home capability, with which citizens go on to the force specific website and complete a form to report a crime as well as force specific other matters (e.g. road collisions and missing persons). Whilst the level of automation differs across forces in the region, forms are either automatically transferred to the Records Management system (Athena) via iHub Online Crime Integration or a copy of the forms are emailed to Contact Management teams for manual review and entering on the appropriate system. Once on the appropriate system, contact is made with the citizen by email or telephone for additional clarification (if required), and an SMS sent manually to provide pertinent information (e.g., reference number, victim support information and/or further supporting information if required), however, the SMS cannot be replied to by the Citizen.

To obtain updates on reports as they are progressed by the force, members of the public rely on manual telephone/email updates from Investigating Officers by telephone or ringing Contact Management on 101 or 999 to request an update or be transferred to their Investigating Officer.

2.5.2. Victim Self-Service Future State: User Journey and/or Citizen Portal

LOT 1: User Journey

Automated, configurable communications via SMS or email using pre-defined rules/data triggers to provide information to members of the public following contact with a force, allowing them to be kept informed of the progress of their interactions in line with Victims Code of Practice (VCoP). The communications could include, but would not be limited to:

- Officer arrival times
- Appointment reminders
- An automated Incident/Crime reference number
- Link to sign up for a Citizen Portal account
- Details of Investigating Officer or changes to Investigating Officer
- Updates on case progression and status
- Victim Support information
- Crime prevention and/or crime scene advice (where relevant)
- Clickable links to view more information
- Opt-out function
- Surveying tools
- Confirmation of or change to court dates
- Court outcomes

LOT 2: Citizen Portal

Members of the public can access a secure and easy to use personal portal to self-serve status updates for crime reports made to a force and access other relevant information. The portal must be capable of integrating into local and national systems/processes and have two-way communications functionality that enables a member of the public and Investigating Officer to request or provide information.

2.6. (2) Customer Relationship Management (CRM)

2.6.1. CRM: Current State

Currently, the tools and systems used for Contact Management do not support force's internal strategies of being efficient and effective. Initial scoping has suggested there are opportunities to improve the Citizen experience when members of the public need to contact a force.

2.6.2. LOT 3: CRM: Future State

Forces are keen to explore the latest technologies (including AI and robotics) that better support an improved customer experience and yield efficiency and effectiveness benefits. The solution may include an improved telephony journey for members of the public which could help to prioritise their need to ensure they are quickly connected with the right person at the right time. This would subsequently reduce the need for members of the public to repeat information, allowing them to contact forces in a variety of ways and across channels (digital and non-digital). Contact Management colleagues would be better equipped to efficiently and effectively manage the ever-increasing demand, and Supervisors will have time to focus on what truly matters.

It is recognised that due to the size of potential change, implementation of a Customer Relationship Management solution would likely require multiple stages.

2.7. It should be noted that forces should have the option to purchase each Lot separately, altogether or as part of a phased adoption.

3. Benefits and Key Performance Indicators

3.1. Benefits

The anticipated benefits associated with the solution(s) are outlined in Table 1.

Benefit Description		User Journey	Citizen Portal	CRM
Reduction in 999 call demand	Tangible	✓	✓	✗
Reduction in 101 call demand	Tangible	✓	✓	✗
Reduction in 101 channel demand*	Tangible	✓	✓	✓
Reduction in 999 and 101 call wait times	Tangible	✓	✓	✓
Improved Contact Management productivity	Tangible	✓	✓	✓
Improved 'Responding to the Public' PEEL Assessment	Tangible	✓	✓	✓
Reduced crime investigation Outcome 16s**	Tangible	✓	✓	✗
Improved Contact Management morale	Tangible	✓	✓	✓
Reduced Contact Management attrition	Tangible	✓	✓	✓
Improved Victims Code of Practice compliance	Tangible	✓	✓	✗
Reduced average time for Officers to update Victims	Tangible	✓	✓	✗
Improved public trust	Tangible	✓	✓	✓
Improved public confidence	Tangible	✓	✓	✓
Improved victim satisfaction	Tangible	✓	✓	✓
Improved Victim Support service awareness	Tangible	✓	✓	✗
Reduction in call prioritisation times	Tangible	✗	✗	✓
Reduction in dispatch times	Tangible	✗	✗	✓
Reduction in response arrival times	Tangible	✗	✗	✓
Improved resource management	Intangible	✓	✓	✓
Reduced risk of human error	Intangible	✓	✓	✓
Improved risk management/decision making	Intangible	✗	✗	✓
Improved interoperability with services/ systems	Intangible	✗	✓	✓

Table 1

**Webchat, Single Online Home, and Social Media Channels*
***Named suspect identified but the victim does not support or has withdrawn from Police action*

3.2. Key Performance Indicators

3.2.1. User Journey Key Performance Indicators

- Reduction in the number of 101 calls where victims are contacting for an update on their crime - KPI of at least 50% 12-months post implementation, with at least a further 20% reduction in Year 2 based on results achieved at the end of Year 1.
- Reduction in the number of 999 calls where victims are contacting for an update on their crime - KPI of at least 50% 12-months post implementation, with at least a further 20% reduction in Year 2 based on results achieved at the end of Year 1.

Key performance indicators in relation to Victims Code compliance and Victim satisfaction to be jointly agreed between the supplier and individual forces as the contract progresses and data availability matures.

3.2.2. Citizen's Portal Key Performance Indicators

- Citizen's Portal to have an availability rate of 99.99%.

  Additional Citizen's Portal Key Performance Indicators will be developed as the front-end of the portal is built by the National Digital Public Contact team (additional details in 5.2).

3.2.3. Customer Relationship Management Key Performance Indicators

- Realise efficiencies to support Contact Management colleagues in being more readily available to answer calls.

- Increased volume of Citizens correctly identified as vulnerable (percentage of citizens to be agreed with forces based on individual service level agreements) within the first 12-month post implementation and the target percentage of citizens correctly identified as vulnerable to be maintained for each subsequent year of the contractual agreement.

- Reduction in Contact Operator 'not ready' time between calls by 50% within the first 12-months post-implementation.

3.2.4. KPIs listed for each of the Lots are indicative and would be subject to ratification with each force prior to contract signature.

4. LOT 1: User Journey

4.1. User Journey Scope and Integrations

4.1.1. User Journeys refer to automated communication via SMS or email using pre-defined rules/data triggers to provide information to members of the public (victims) following contact with the police, allowing them to be kept informed of the progress of their interactions with the force through automated, configurable messaging.

4.1.2. Each force is likely to require approximately between eight and ten 'journeys,' consisting of both 'standard' and 'enhanced' journey types. It should be noted that the estimated number of journeys should be used as a guide only and is no guarantee of volume under this contract.

4.1.3. **Standard Journey** = the journey will be the same irrespective of the crime/incident type, as long as it meets a force's inclusion criteria (inclusion criteria will differ for each force). The 'journey' is likely to be determined by the incident grading applied by the Contact Management colleague. For example, in Bedfordshire, incidents are graded as Immediate, Prompt, Scheduled, Appointment or No Response, dependent on the assessment of threat, harm and risk. This means there is likely to be approximately five 'standard' journeys. It should be noted that not all forces will use the same incident grading categories.

4.1.4. **Enhanced Journey** = the journey will differ to a 'standard' journey and be determined by an agreed crime/incident type, irrespective of the incident grading applied by the Contact Management colleague.

Enhanced journeys are likely to focus on force's higher demand crime types/incidents or force priorities and provide bespoke SMS/email communications relating to that crime type.

4.1.5. An example of a standard and enhanced journey can be found in Appendix 1.

4.1.6. The volumes of SMS/emails to a member of the public as part of a given 'journey' is likely to differ between each force dependent on:

1. Whether forces opt to implement the Citizen Portal solution alongside the User Journey (without a portal, forces may choose to design their journeys to include poignant status updates for reports that would otherwise have been self-serviced via a portal account).
2. Individual force inclusion/exclusion criteria (e.g., exclusion of crime/incident types, vulnerability markers, ages, or witnesses),
3. Changes to force inclusion/exclusion criteria throughout the duration of the contract,
4. Force's volume of crimes/incidents that meet their inclusion criteria, which may fluctuate during certain periods (e.g., increase in burglaries during winter months),
5. The number of journeys designed by each force and the number of automated communications messages each journey itself.

4.1.7. To support pricing proposals, it is proposed that bidders use the total number of crimes recorded by each force across a 12-month period and apply the assumption that each of those crimes will require a journey consisting of approximately five SMS/emails.

4.1.8. For example, a total of 51,532 crimes were recorded by Bedfordshire Police between June 2023-2024. Using the assumption that each reported crime will have a 'journey' consisting of approximately five automated communication messages, means Bedfordshire Police would send approximately 257,660 automated messages per year.

4.1.9. Data taken from the Office of National Statistics highlighting the total number of recorded crimes (excluding Fraud offences) between June 2023-June 2024 for each force in the Eastern Region can be found below. It should be noted that these volumes are based on historical demand and should only be used as a guide. The information is no guarantee of volumes under this contract as these may fluctuate based on the variables referenced in 4.1.6.

Bedfordshire = 51,532
Cambridgeshire = 68,580
Hertfordshire = 75,288
Norfolk = 59,228
Suffolk = 46,027
Kent = 164,945
Essex = 151,967

4.1.10. The User Journey solution will require integration with force's Command and Control and Record Management Systems and their associated governance boards. The Command-and-Control system currently used across the Eastern Region is a combination of SMARTStorm and STORM MA (all forces are expected to migrate to SMARTStorm by December 2026), provided by Sopra Steria. Whilst the system is the same across the Eastern Region, each force uses different features and consequently, there is not a standard build which may result in differing data trigger points, requiring the supplier to be adaptable.

4.1.11. The Record Management System used by all forces in the Eastern Region is currently a standard build of Athena (CONNECT), provided by NEC, however the supplier must be adaptable as this may change throughout the duration of the contract.

4.1.12. It should be noted that Athena is a shared system across nine-forces, making up 30% of Policing across England and Wales. As a result, there is a strict governance process in place to ensure that the shared platform is not compromised by the introduction of any new capability. Early scoping has suggested that a supplier may need to connect to a force's data warehouse (which stores copies of force's Athena data and has a 'read only' capability), as an interim whilst approval to interface with Athena is sought through the governance process. Each force has its own data warehouse, which stores differing data, therefore bidders should consider whether there would be a cost implication to connect to a force's data warehouse prior to connecting to Athena directly at a later date if approved through the governance process.

4.2. User Journey Detailed Functional Requirements

4.2.1. The functional requirements for the User Journey solution are outlined in Table 2.

4.2.2. Each requirement has been assigned a MoSCoW priority rating for the development phase:

- 'MUST have' requirements are critical to meet business needs.
- 'SHOULD have' requirements are needed but not as critical as the MUST requirements.
- 'COULD have' requirements are optional/are not essential.

ID	Description – Business Functional Requirement	Priority
1	Solution must be available 24/7, 365 days a year.	Must
2	Comply with the latest version of Web Content Accessibility Guidelines (currently 2.2).	Must
3	Ability to comply with force policies in relation to the Review, Retention and Deletion of information to ensure compliance with the Police Information and Records Management (PIRM) Code 2023.	Must
4	Ability for forces to send a series of automated SMS/email communications following contact by a MoP at agreed intervals using pre-defined rules and data triggers from the Force's Command & Control and/or Record Management System. Note: these will be able to differ for each force.	Must
5	Where the Service will be used across multiple forces, the Supplier should describe how access to data can be restricted on a force per force basis – but also how the data can be shared between forces where appropriate.	Must
6	MoP will have the ability to opt out of receiving automated communications.	Must
7	Forces will be able to define their own inclusion/exclusion criteria for automated communications and update the eligibility list as required.	Must
8	Ability to schedule SMS/emails to a MoP to ensure messages are not sent during unsociable hours where appropriate. The notification schedule must be configurable.	Must
9	Automatic entries will be made into the force's Command & Control system, detailing the time/date and content of all SMS/email communications with a MoP whilst the corresponding Command & Control system log is open.	Must
10	Automatic entries will be made into the force's Record Management System, detailing the time/date and content of all SMS/email communications with a MoP after an incident has been crimed and there is a crime record.	Must
11	MoP will have the ability to follow links provided to them by the force in the automated communications, e.g., to access information on local force websites.	Must
12	Ability for forces to change brand and logo in the automated communications.	Must
13	Ability to report on the number of SMS and email communications that have been sent by SMS/email template title and crime/incident type.	Must
14	Ability to report on the specific dates/times that SMS, and emails have been sent to MoP by SMS/email template title and crime/incident type.	Must

15	Ability to identify and report whether SMS and emails are delivered/undelivered by SMS/email template title and crime/incident type.	Must
16	Ability to feed reports into relevant force PowerBI dashboards.	Must
17	Suppliers must keep a record of actions taken against a problem or incident and make these available to force(s) upon request.	Must
18	The solution will enable authorised users to easily modify content through an intuitive and user-friendly interface, without requiring specialised technical knowledge or coding skills.	Must
19	Ability for messages to be translated into different languages to suit a MoP language preference.	Should

Table 2

4.3. User Journey Deliverables and Timescales

4.3.1. Indicative milestones, deliverables, and estimated timescales for the delivery of a User Journey solution are outlined in Table 3. Final timelines and deliverables will be confirmed once a supplier has been identified.

Milestone	Deliverables	Approximate Timescale *(post contract award)*
Project Initiation	• Mobilisation of resources • Detailed Project Plan, including timelines.	Week 1-2
Detailed Requirements Gathering and Analysis	• Completion of user, system, and data requirements documentation	Weeks 3-5
System Design and Architecture	• High level system design specification, including technical architecture and integration plans. • System design and architecture approval.	Weeks 5-8
System Development	• Completion of core system development • Testing plans	Weeks 8-12
Testing and Quality Assurance	• Systems Integration Testing • User Acceptance Testing • Information Assurance/Security Testing • Final Acceptance Approval	Weeks 8-13
Deployment	• System deployment • Solution Design Document updated and handed over to appropriate Team.	Week 14
Post-Deployment Support	• On-going support post deployment • Hypercare period • Measurement and tracking of solution.	Week 15+

Table 3

4.3.2. Each milestone is to be reviewed and approved through the agreed governance channels before proceeding to the next phase. Delays or deviations from the agreed timescale tolerances will require a written exception report detailing the cause of the deviation (either predicted or actual), consequences, mitigation strategies, available options, and the required decision.

4.4. User Journey Aftersales Support

4.4.1. Indicative response and target resolution times are outlined in Table 4.

- Support will be available for critical and high priority incidents 24/7 via telephone support number and a support portal.
- Support will be available for medium and low priority incidents between 8am-5pm on UK working days via a support number, email, and/or a support portal.

Priority	Response Time	Target Resolution	Description
Critical	15 Minutes	Within 4 hours	Serious issue – business is not able to function.

High	2 Hours	Within 1 Working Day	Significant impact but business is able to function.
Medium	1 Working Day	Within 3 Working Days	Small impact to the business but issue can be circumvented.
Low	3 Working Days	Within 10 Working Days	Negligible impact to the business.

Table 4

- Change Management process to be provided and forces to be notified in advance of any regular maintenance, including expected downtime and testing conducted to minimise disruption to users and enable forward planning where required. The supplier should also notify forces of emergency change with as much notice as possible to enable impacts on business provisions to be established.
- Problem Management process to be provided with expected timescales for development and release of defect fix patches (for example quarterly).
- The supplier must detail their hardware replacement programme and any impact on project delivery.
- Monthly reporting and service review meetings.
- Service Level Agreement detailing the support process. This will be reviewed by forces prior to contractual agreement to ensure it includes a breakdown of service level agreements, support phone number, email address and portal links, escalation details and penalties if service level agreements are not met.
- Forces should also have the option to opt for a 'managed service' and suppliers should provide pricing structures around the cost for a 'managed service' and any continual service improvement.

5. LOT 2: Citizen Portal

5.1. Citizen Portal Scope and Integration

5.1.1. The portal will allow a member of the public to track their case as it is progressed by the police and enable direct two-way communications between the member of public and the assigned Investigating Officer up until the point of charge.

5.1.2. The initial scope of the portal is summarised below:

- Secure access for a member of the public.
- Track status updates for crimes *(inclusion criteria for each force to be locally agreed).*
- Two-way communications between a member of the public and the assigned Investigating Officer.
- Access to and provision of relevant additional information.

5.1.3. The Citizen Portal solution will require integration with forces' Command and Control and Record Management Systems, which will be subject to force governance boards. The Command-and-Control system currently used across the Eastern Region is either SMARTStorm or STORM MA, which are two generations of the same system both developed and supported by Sopra Steria (all forces are expected to be on the SMARTStorm version by December 2026). Whilst the system is the same across the Eastern Region, each force uses different features and consequently, there is not a standard build which may result in differing data trigger points, requiring the supplier to be adaptable.

5.1.4. The Record Management System used by all forces in the Eastern Region is currently a standard build of Athena (CONNECT), provided by NEC, however the supplier must be adaptable as this may change during the contract.

5.1.5. Athena is a shared system across nine-forces, making up 30% of Policing across England and Wales. As a result, there is a strict governance process in place to ensure that the shared platform is not compromised by the introduction of any new capability. Early scoping has suggested that a supplier may need to connect to a forces' data warehouse (which stores copies of force's Athena data and has a 'read only' capability), as an interim whilst approval to interface with Athena is sought through the governance process. There are a number of data warehouses across the Athena forces, each of which store differing data; therefore, bidders should consider whether there would be a cost implication to connect to a force's data warehouse as an interim and connecting to Athena directly at a later date if approved through the governance process.

5.2. Citizen Portal Detailed Functional Requirements

5.2.1. The Digital Public Contact team have been consulted regarding the Citizen's portal functional requirements to ensure an Eastern Region portal solution is interoperable with, and allows for, integration with the National *MyPolice* portal.

5.2.2. Each requirement has been assigned an ID, Component Category, MoSCoW priority and delivery phase for development.

5.2.3. **ID Reference:**
A unique number and format assigned to each requirement.

5.2.4. **Component Category:**
Figure 1 provides a high-level overview of the generic architecture of an end-to-end portal product, of which the National component 'front-end' will be provided by the National Digital Public Contact Programme and the Force component 'back-end' will be procured by local force(s) as part of this procurement process to enable integration and interoperability. To support suppliers in providing a pricing proposal for the 'back-end' components, each functional requirement has been assigned a component category.

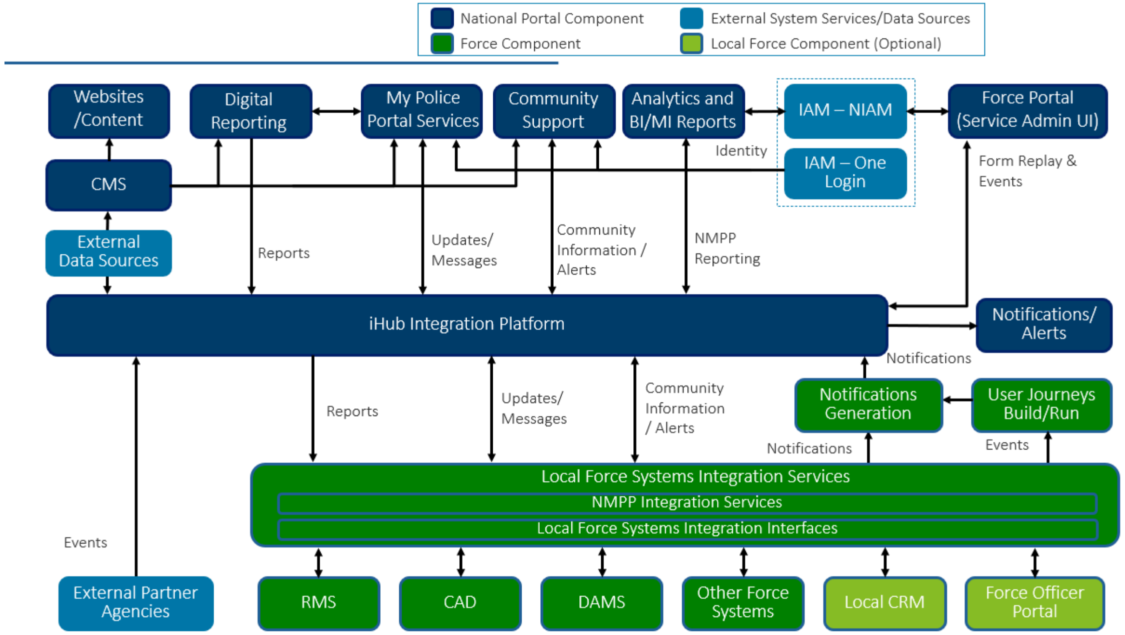
National Portal Component
External System Services/Data Sources
Force Component
Local Force Component (Optional)
Websites /Content
Digital Reporting
My Police Portal Services
Community Support
Analytics and BI/MI Reports
IAM – NIAM
Force Portal (Service Admin UI)
Identity
IAM – One Login
Form Replay & Events
CMS
External Data Sources
Reports
Updates/ Messages
Community Information / Alerts
NMPP Reporting
iHub Integration Platform
Notifications/ Alerts
Notifications
Reports
Updates/ Messages
Community Information / Alerts
Notifications Generation
User Journeys Build/Run
Notifications
Events
Local Force Systems Integration Services
NMPP Integration Services
Local Force Systems Integration Interfaces
Events
External Partner Agencies
RMS
CAD
DAMS
Other Force Systems
Local CRM
Force Officer Portal

Figure 1

National Component (Front-end):

Component Name	Description
Websites/Content and Content Management System	Existing SOH services built on Optimizely (formerly EPiServer) content management system CMS (v11), implemented with an Infrastructure as a Service (IaaS) architecture on Azure cloud.
Digital Reporting	Existing services that allow the public to submit crime and non-crime reports, including road traffic incidents, firearm licenses, etc.
MyPolice Portal Services	My Police Portal (MPP) service allows members of the public (MoP) to track case status and engage directly with a Police Officer or Staff member (via two-way messaging). It also allows for the uploading and exchange of files and text-based information and provides access to additional information.
Community Support	A national capability that provides localised community information and drives engagement with the police on community issues. This ensures a single, trusted police voice for the public.
Analytics and BI/MI Reports	A national capability that allows force users to analyse NMPP data through standard and bespoke reports, including the ability to export the data. This data can then be shared with the DPC National Analytics and Insights view.
Identity & Access Management (IAM)	The preferred solution for Identity and Access Management (IAM) is to leverage the GOV.UK One Login service to manage the identity of MoP and NIAM to manage the identity of Force users.
iHub Integration Platform	A national integration platform that captures, transform, and routes data between front-end components and force back-end systems.
Notifications and Alerts	A notifications and alerts service delivers notifications (email, SMS) to Members of Public (MoP). This notification and alert services support system and force generated notifications and delivers them to the MoP over their preferred channel (Email, SMS).
Force Portal (Service Admin UI)	A Digital Public Contact (DPC) developed service management component enabling Force users (Force Admins) to replay, re-route, and download relevant submissions. The Force portal to include a national administration UI enabling service management users (administrators) to manage National My Police Portal services.

Force Component (Back-end):

Component Name	Description
Local Force Systems Integration Services	A local integration platform leveraging API management capabilities within existing products or a purpose-built solution to enable connectivity with Force IT systems. This includes Integration services required to connect NMPP solution with the Force system integration interfaces and integration interfaces to enable data connections with Force IT systems (RMS, CAD, and DAMS etc.)
Record Management System (RMS)	A system of record for Forces, supporting Officer in Case (OIC) case reviews and two-way messaging (depending on RMS vendor capabilities).
Command and Control (CAD)	A Force Command and Control system captures and records incidents and includes other functionalities such as dispatching officers.
Digital Asset Management System (DAMs)	An asset management system for forces to receive, store, manage and share digital assets in relation to both crime and non-crime matters.
Other Force Systems	Other key systems used by forces for other crime and non-crime workflows including systems such as Compact, CRaSH, NFLMS, Centurion, etc.
Local CRM	An optional system to support MoP relationship management. A required component to support portal services such as Witness Care etc.
Force Officer Portal	An optional force portal service that allows forces to efficiently assess, respond to, and triage MoP communications and operational services of the NMPP.
User Journeys Build/Run	Force capability for defining user journey workflows and determining required notifications, driven off Force system events. only a limited number of forces providing these services locally. Only a limited number of forces provide this service locally.
Notifications Generation	Force capability to generate notifications to the public, delivered via Victim Journey or iHub Platform etc., driven by the workflow triggers from the force systems.
External Partner Agencies	Partner agencies work closely with the forces. Integration with their systems will support collaboration and efficient case management.

5.2.5. Phases

A breakdown of the initial scope of requirements into Phase 1, Phase 2, and Future. The Digital Public Contact Team anticipate delivery of the Phase 1 front-end requirements by June/July 2025, coinciding with the Eastern Region procurement timelines. There is currently no timescale for the delivery of the Phase 2 and Future requirements, but once this is known, the information will be shared with the Supplier.

5.2.6. MoSCoW priority rating definitions:

- 'MUST have' requirements are critical to meet business needs.
- 'SHOULD have' requirements are needed but not as critical as the MUST requirements.
- 'COULD have' requirements are optional/not essential.

5.2.7. Business Functional Requirements

Front-end requirements will be provided by the Digital Public Contact Team but have been included in the functional requirement set for transparency. Suppliers will only be required to provide costings for the 'front-end and back-end' and 'back-end' requirements.

ID	Component Category	Description – Business Functional Requirement	Phase	Priority
		General		
1	Front-end	Ability for forces to change brand, i.e., logo and colours.	Phase 1	Must
2	Front-end & Back-end	Solution must be available 24/7, 365 days a year.	Phase 1	Must
3	Front-end	Comply with the latest Web Content Accessibility Guidelines (WCAG), currently 2.2.	Phase 1	Must
4	Back-end	Ability to comply with force policies in relation to the Review, Retention and Deletion of information to ensure compliance with the Police Information and Records Management (PIRM) Code 2023.	Phase 1	Must
5	Front-end & Back-end	Where the Service will be used across multiple forces, the Supplier should describe how access to data can be restricted on a force per force basis – but also how the data can be shared between forces where appropriate.	Phase 1	Must
		Enrolment and Authentication		
6	Back-end	The forces will initiate an invitation for eligible MoP to enrol via an SMS or email sent through the integration layer that will allow them to create a Portal account.	Phase 1	Must
7	Back-end	The forces will trigger reminders to be sent to the MoP if they have not accepted the 'Invitation to Register' within an agreed period.	Phase 1	Must
8	Front end	The portal will allow notifications to be sent to forces when a MoP has registered for a portal account.	Phase 1	Must

9	Back-end	Forces will be able to define their own inclusion/exclusion criteria for a MoP to receive a portal link and update the eligibility list as required.	Phase 1	Must
10	Front-end	The MoP will be able to register for a portal account in the English language.	Phase 1	Must
11	Front-end	MoP will be able to set preferences for notifications during account creation and edit these at any time.	Phase 1	Must
12	Front-end	Ability for MoP to create an account, including secure log in detail creation (username, password and multi factor authentication details).	Phase 1	Must
13	Front-end	The portal will display relevant terms and conditions, data protection and cookies policies a MoP to read and accept when creating an account.	Phase 1	Must
14	Front-end	The portal will allow the MoP the option to configure a number of MoP characteristics, such as age and diversity information during account creation.	Phase 2	Must
15	Front-end	The portal will work with the selected Identity Provider to ensure an email verification is sent to the MoP to verify that their email address used in the account creation is valid and controlled by the user requesting account registration.	Phase 1	Must
		Sign In		
16	Front-end	The portal will allow a registered MoP to sign in to their account by entering their identity details created during the registration process (sign in credentials).	Phase 1	Must
17	Front-end	The portal will validate the registered MoP account with multi-factor authentication.	Phase 1	Must
18	Front-end	The portal will perform an authentication check every time a registered MoP signs into their portal account.	Phase 1	Must
19	Front-end	The portal will allow the MoP to use all portal services by logging into the portal with one set of account details throughout their user journey (e.g., Single Sign On).	Phase 1	Must
20	Front-end	The portal will automatically log out the MoP after a period of inactivity within an open session.	Phase 1	Must
21	Front-end	The portal will be accessible via a web link only after successful enrolment.	Phase 1	Must
		Access		
22	Front-end	The portal will allow the MoP to access SOH reporting and all SOH existing advice and information.	Phase 1	Must
23	Front-end	The portal will allow the MoP to access the portal in English language.	Phase 1	Must
		Self-Account Management		
24	Front-end	MoP will be able to reset their portal account details at any time through the Identity Provider/portal services.	Phase 1	Must

25	Front-end	MoP will be able to view/edit their notification settings at any time.	Phase 1	Must
26	Front-end	MoP will be directed to self-help if they are unable to submit changes to their account settings.	Phase 1	Must
27	Front-end	MoP will be sent a notification when there have been changes made/saved to any of their account settings.	Phase 1	Must
28	Front-end	The portal will allow the MoP to view their account profile containing but not limited to account Information including personal details and notification setting preferences.	Phase 1	Must
29	Front-end	The portal will allow the MoP to view/edit their Account Information, including but not limited to first name, last name, current address, email, and phone number.	Phase 1	Must
30	Front end	The portal will detect and identify any changes to a member of the public's account information and notify all relevant forces of the change through the integration layer. This applies regardless of the source of the change, whether it originates from: • A system of record, or • The MoP changing their personal data in their portal account.	Phase 1	Must
31	Back-end	The force integration services will handle notifications of changes of personal data for a MoP as follows: • Any changes notified by the portal will update the appropriate force system of record, accordingly, including new, changed or deleted information.	Phase 1	Must
32	Front-end & Back-end	The portal will identify a change that has been made to a defined set of the Account Information (personal details), and any forces with live contacts will be informed of those change details.	Phase 2	Must
33	Front-end	The MoP will be able to delete their portal account.	Phase 1	Must
34	Front-end	MoP will be able to manage their account in English language.	Phase 1	Must
35	Front-end	The portal will create the association with the designated individual (witness, parent/guardian, attorney) and the case (system of record) received through the integration layer.	Phase 1	Must
36	Front-end	The portal will allow the designated individual with an assigned role (witness, parent/guardian, attorney) to view the linked case information instead of or in addition to the victim.	Phase 1	Must
37	Back-end	The force systems will identify and link specific roles (victim, witness, parent/guardian, attorney) to cases (i.e. crime records) and send the case details (including linked roles) to the portal through the integration layer.	Phase 1	Must
38	Back-end	The force systems will send an enrolment link to the designated individuals (witness, parent/guardian, attorney) that will allow them to create a portal account.	Phase 1	Must

39	Front-end	The portal will allow the MoP to manage a portal account on behalf of others, to nominate/add others and remove/transfer control.	Phase 2	Must
40	Front-end	The portal will allow the creation of an association between a MoP and one or more organisations (e.g., their business, workplace, a charity organisation, or social club) and will provide capabilities to set, and ratify, their role within the organisation, based on an agreed set of constrained values (e.g. employee, manager, administrator) , for any record, for any in-scope system of record, such as a crime received through the integration layer. The MoP and any person with the appropriate assigned role within that organisation will be able to update/delete their associations at any time.	Phase 2	Must
41	Front-end	The portal will allow a MoP with the assigned role within an organisation to view and manage all nominals associated with that organisation, including changing their role, ratifying their roles, and removing them from the organisation.	Phase 2	Must
42	Back-end	The force systems will identify and link specific associations (e.g., business, workplace, a charity organisation or social club) to cases (i.e. crime records) and send the case details (including linked associations) to the portal through the integration layer.	Phase 2	Must
43	Back-end	The force systems will initiate an invitation to the designated individuals with specific associations (e.g., business, workplace, a charity, organisation or social club) that will allow them to create a portal account.	Phase 2	Must
		Portal Accounts and Permissions		
44	Back-end	The force can add/update/remove user permissions.	Phase 1	Must
45	Back-end	The force will have the ability to define Administrators for the portal.	Phase 1	Must
46	Back-end	The force administrators will be able to provide support to portal users ensuring they have suitable access (e.g., block portal accounts if required).	Phase 1	Must
47	Front-end	The portal system will validate force user details in line with force defined role-based access control and permissions when they log-in to the portal admin area.	Phase 1	Must
48	Front-end & Back-end	Available via Web performing consistently across different devices and operating systems with reliability rate of 99.99% with 0% data loss.	Phase 1	Must
49	Front-end & Back-end	The portal will allow authorised force users to access portal information under relevant system access management and control processes.	Phase 1	Must
50	Back-end	Provide visibility to internal users as to whether accounts are held or not for MoP.	Phase 1	Should
50a	Back-end	The force systems will link all new system of records (reported crimes and incidents) to a MoP's portal account (One Login sub-ID) if a portal account already exists for the MoP.	Phase 1	Must

50b	Back-end	The force systems will initiate a notification only (not an invitation) to the MoP with an existing portal account for new system of records.	Phase 1	Must
50c	Front-end	The portal will send notifications only (not an invitation) to the MoP with an existing portal account when a new system of record (reported crimes and incidents) is received via the integration layer.	Phase 1	Must
		Track Case Progress		
51	Front-end	MoP will be able to view live data from within their portal account.	Phase 1	Must
52	Front-end	MoP will be able to view historic data from within their portal account.	Phase 2	Must
53	Front-end	MoP will be able to view and select each of their reported cases with the force from the portal.	Phase 1	Must
54	Front-end & Back-end	MoP will be able to see case details for each reported case with the force, in line with force(s) inclusion/exclusion criteria (including Investigating Officer, case status, associated messages, crime reference and case timeline) by reading Record Management System data.	Phase 1	Must
55	Front-end	MoP will have a personalised dashboard showing all cases they have reported, including but not limited to high level case status and when they last logged in.	Phase 1	Must
56	Back-end	Forces will be able to determine how frequently changes to any of the case details for each reported case with the force (including OIC, case status, associated messages, crime reference number and timeline of case) will be available to the MoP from within their portal account. The frequency of these updates will be able to differ dependent on the information they relate to (e.g., data refresh in the portal may differ for OIC when compared to case status).	Phase 1	Must
57	Front-end	MoP will be able to download their reported case details into a PDF file.	Phase 1	Should
58	Front-end	MoP will be able to see which of their reported cases with have updates/alerts from within the portal.	Phase 1	Must
59	Front-end	MoP will be able to see any associated appointments that have been booked by the force for their reports from within their portal account.	Future	Should
60	Back-end	Forces will be able to configure what information is displayed to a MoP from their portal account.	Phase 1	Must
61	Back-end	Ability for the portal to identify cases eligible for auto updates on case progress, in line with force(s) agreed inclusion/exclusion criteria.	Phase 1	Must
62	Back-end	Forces must be able to configure if/when a MoP will receive a notification regarding an update on their case (e.g., change in status).	Phase 1	Must
63	Front-end	The portal will be able to provide notifications for status updates in English.	Phase 1	Must
64	Back-end	Ability to schedule notifications to a MoP to ensure messages are not sent during unsociable hours where appropriate. The notification schedule must be configurable.	Phase 1	Must

65	Back-end	The portal must notify the force users when interactions are dictated by policy, legislation (i.e., VCoP standard/enhanced victims and statutory time limits) or as agreed with the MoP (i.e., Victim Contract) are due.	Phase 1	Must
66	Front-end & Back-end	The portal will flag cases which are unsuitable for an auto-update and notify forces to review and manage them.	Phase 2	Must
67	Front-end	The portal will allow forces to review details including but not limited to, whether the MoP has an account, whether they are an individual or nominated person in relation to status updates, how the contact was made by the Mop and case reference number.	Phase 2	Must
		Community Messages and Services		
68	Front-end & Back-end	Ability for MoP to view information relating to crimes in their area from their portal account specific to MoP active location and in line with their preferred location.	Phase 2	Must
69	Front-end & Back-end	Ability for MoP to receive notifications from the force to the community, including incident alerts, to their chosen channel of communication.	Phase 2	Must
70	Front-end & Back-end	Ability for a force to tailor notifications based upon data available. E.g., crime prevention advice sent to surrounding area with increased theft.	Phase 2	Must
71	Front-end & Back-end	Ability to display community support based on a MoP location.	Phase 2	Must
72	Front-end	Ability for MoP to change their location preferences.	Phase 2	Must
73	Front-end	The portal will allow the MoP to access SOH 'Your Area' via the portal.	Phase 1	Must
74	Front-end	Ability for MoP to customise community information categories they want to receive and set notifications/alerts.	Phase 2	Must
75	Front-end	MoP will be able to use links within their Portal account to access the Single Online Home platform and navigate to the required information.	Phase 1	Must
		Two Way Communications		
76	Front-end	MoP will be able to have two-way communications with their Investigating Officer from their portal account for their reported incidents.	Phase 1	Must
77	Front-end	MoP will be able to send messages in English.	Phase 1	Must
78	Back-end	The portal will allow the force user to view whether a MoP has an account in relation to the two-way communications. Note: To be viewable in the force RMS.	Phase 1	Must
79	Back-end	The portal system will allow the force users to view guidelines on sending messages.	Phase 1	Must
80	Back-end	The portal system will allow the MoP to view guidelines on sending messages and receiving responses.	Phase 1	Must

81	Front-end	MoP will only be able to send messages to their Investigating Officer is the investigation status is 'open' – functionality to be disabled for closed reports.	Phase 1	Must
82	Back-end	Force user will only be able to send messages to the MoP if the case status is 'open' - functionality to be disabled for closed cases.	Phase 1	Must
83	Front-end	MoP will receive a confirmation message once their message has been sent.	Phase 1	Must
84	Back-end	Ability to identify if a MoP is reporting a new crime in their message to an Investigating Officer via the portal.	Phase 1	Must
85	Front-end	Ability to signpost MoP to the correct place to report a new crime/incident to the force.	Phase 1	Must
86	Front-end	Ability to provide guidance to a MoP to manage expectations about Investigating Officer responses to their queries.	Phase 1	Must
87	Back-end	Automatic entries will be made into the force's Record Management System, detailing the time/date and content of all SMS/email communications sent by a MoP from the portal to their Investigating Officer and it will allow force users to receive and review messages sent by the MoP within a managed task list.	Phase 1	Must
88	Back-end	Investigating Officers will receive automated notifications when a MoP submits a new message via their portal account.	Phase 1	Must
89	Back-end	Ability to provide Investigating Officers with suggested responses to MoP messages that can be manually edited/updated.	Phase 1	Could
93	Back-end	Ability to provide 'suggested actions' for an Investigating Officer tailored dependent on the nature of a MoP message.	Phase 1	Could
94	Back-end	Investigating Officers will be able to send messages to the MoP, including but not limited to, pre-populated messages, single messages, or free text, relating to their case, or reply to messages sent by a MoP.	Phase 1	Must
95	Front-end & Back-end	The portal will allow forces to request a 'read receipt' from the MoP.	Phase 2	Must
96	Front-end & Back-end	The portal will allow the MoP to receive and accept a read receipt sent by the force.	Phase 2	Must
97	Back-end	Capability to change/recall messages sent by an Investigating Officer to a MoP portal account.	Phase 1	Should
98	Front-end & Back-end	A copy of the messages sent by an Investigating Officer to a MoP will automatically stamp into the portal for a MoP to view (including content and time message sent).	Phase 1	Must
99	Front-end	MoP will be sent a notification when they have a new message from an Investigating Officer in their portal account.	Phase 1	Must
100	Back-end	Ability to schedule notifications of a new message from an Investigating Officer to a MoP so as messages are not sent during unsociable hours where appropriate. The notification schedule must be configurable.	Phase 1	Must
101	Back-end	Automatic entries will be made into the force's Record Management System, detailing the time/date and content of all SMS/email communications sent by an Investigating Officer to a MoP via the tool, enabling contact to form part of the case file and Investigating Officers/Supervisors to view.	Phase 1	Must

102	Front-end	MoP will be able to view their sent messages and manage them as required (e.g., mark as read/unread, open and delete (soft delete)).	Phase 1	Must
103	Front-end	The portal will allow the MoP or Force to re-attempt sending a message for up to a maximum number of attempts, signposting them to the in-tool guidance if unsuccessful.	Phase 1	Must
104	Back-end	Ability to automatically escalate MoP messages to Supervisors if an Investigating Officer has not responded within defined timescale.	Phase 1	Must
105	Back-end	Investigating Officers will be able to add an update to the Record Management System without triggering an update to be sent to a MoP.	Phase 1	Must
106	Front-end	The portal system will contain pre-formatted templates for letters, forms, information requests, or other frequently used documentation in line with force configuration needs (e.g., Victim statements, MG Forms, MoP availability requests, needs assessment forms etc).	Phase 2	Must
107	Front-end & Back-end	The portal will allow the MoP to upload and submit additional **text-based** information / evidence to the reported case upon request by the Force and in line with force process.	Phase 1	Must
108	Front-end & Back-end	The portal will allow the MoP to upload and submit additional **file-based** information / evidence (e.g. video, photo, audio) to their report / submission (crime or non-crime) in line with force process	Phase 2	Must
109	Front-end & Back-end	The portal system will allow the MoP to use digital signatures to support signing of documentation needed to support specific operational use cases (e.g., Victim Statement).	Phase 2	Must
110	Front-end	The portal will send a confirmation to the MoP upon successful submission of the uploaded files.	Phase 2	Must
111	Front-end	The portal will allow re-uploading of the files for a maximum number of attempts, signposting them to the in-tool guidance if unsuccessful.	Phase 2	Must
112	Front-end	The portal will identify which additional evidence/files have been submitted by a MoP via their portal account and notify the respective force through the integration layer.	Phase 2	Must
113	Back-end	The force integration services will upload the additional evidence/files submitted by the MoP via their portal account into their relevant force systems (e.g., Digital Asset Management system).	Phase 2	Must
114	Back-end	Investigating Officers will receive automated notifications when additional evidence/files submitted by a MoP in one of their cases is automatically uploaded to DAMs requesting them to review.	Phase 2	Must
115	Back-end	Additional evidence/files submitted by MoP that is automatically uploaded to DAMs will have a suggested MOPI (Management of Police Information) grading applied (based on available case information such as crime type) for the Investigating Officer to review/approve.	Phase 2	Could
116	Back-end	Investigating Officers will be required to approve the suggested Police Information and Records Management (PIRM) 2023 grading and have the ability to manually override the suggested grading.	Phase 2	Could

117	Back-end	Automated notifications to be sent to an Investigating Officer when additional evidence (video/photo/audio media file) is sent by a MoP for a reported crime, including the link to view the evidence.	Phase 2	Must
118	Front-end & Back-end	Ability for Officers to send additional information to a MoP portal account for one of their reported cases.	Phase 1	Must
119	Back-end	Ability to for an Investigating Officer to extract the conversation in a readable conversation style on word or PDF document that may be used as evidence and/or unused material in a case.	Phase 1	Must
		Automated Summaries		
120	Back-end	Ability to provide automated summaries of Record Management System and Command & Control System data relating to a MoP case for the assigned Investigating Officer to review.	Phase 1	Could
121	Back-end	Ability for assigned Investigating Officers to use AI to ask questions about a MoP in a case to support decision making/safeguarding.	Phase 1	Could
		Interactive Services		
122	Front-end	MoP will be able to access relevant victim support service advice and information relating to the Victim's Code of Practice.	Phase 1	Must
123	Front-end	Ability for a MoP to be able to quickly exit the portal if required.	Phase 1	Must
124	Front-end	The portal will allow MoP data to be used in SOH when the MoP uses the SOH services (e.g., personal details entered during account creation to be pre-populated in SOH forms when the MoP uses the SOH reporting services).	Phase 2	Must
125	Front-end & Back-end	The portal system will validate the MoP message in line with the minimum data specification for the force.	Phase 1	Must
126	Front-end & Back-end	The portal will conduct validation of the files in line with minimum force data specification and send the uploaded files to the force.	Phase 2	Must
		Feedback		
127	Front-end	MoP will be able to provide feedback on the useability and usefulness of the portal.	Phase 1	Must
		Victims Code of Practice		
128	Front-end	The portal will provide information about compensation to the MoP at the appropriate point in their user journey (VCoP Right 5).	Future	Must
129	Front-end	The portal will provide information to the MoP about the prosecution (VCoP Right 6).	Future	Must
130	Back-end	The force system (e.g. CMS/WMS/Athena) will send information about the prosecution to the MoP’s portal account (VCoP).	Future	Must
131	Front-end	The portal will provide the opportunity to the MoP to make a Victim Personal Statement at any point in their user journey (VCoP Right 7).	Future	Must
132	Front-end	The portal system will provide guidance to make a complaint about their Rights not being met (VCoP Right 12).	Phase 1	Must
133	Front-end	The portal system will allow the MoP to self-refer to Victim Support Services for each case in the portal (VCoP Right 4).	Future	Must

134	Front-end & Back-end	Automatic case creation on a force's Victim Support case management system if a MoP self-refers from their portal account.	Future	Should
135	Back-end	Ability to identify duplicate victim support cases (i.e., if a report has already been referred to Victim Support service by the force).	Future	Should
136	Front-end	The portal will provide information to the MoP about the trial (VCoP - Right 8).	Future	Must
137	Back-end	The force system (e.g. WMS/CMS/Athena) will send information about the trial to the MoP's portal account.	Future	Must
138	Front-end	The portal will provide information to the MoP about the outcome of the case and any appeals (VCoP Right 9).	Future	Must
139	Back-end	The force system (e.g. WMS/CMS/Athena) will send information about the outcome of the case and any appeals to the MoP's portal account.	Future	Must
140	Front-end	The portal will provide information to the MoP about the offender following a conviction (VCoP Right 11).	Future	Should
141	Back-end	The force system (e.g. WMS/CMS/Athena) will send information about the offender following a conviction to the MoP's portal account.	Future	Should
142	Front-end	The portal will provide information to the MoP about their Right to Review (including criteria) at the appropriate point in their journey (VCoP Right 6).	Future	Must
		In-Tool Guidance		
143	Front-end	Provision of in-tool / self-help guidance and training for users.	Phase 1	Must
144	Front-end	Users will be referred to the relevant force for help in resolving any errors/issues that cannot be resolved using built-in self-help tools.	Phase 1	Must
		Reporting		
145	Front-end	Ability to identify, monitor and report on portal usage and uptake, including but not limited to: • Number of portal accounts created/used. • Number of visitors to the portal system. • Whether accounts created have any associated activity with them.	Phase 1	Must
146	Front-end	Ability to provide a 'User Experience' report (satisfaction ratings and feedback).	Phase 1	Must
147	Front-end	Ability to allow the authorised force user to search/run and download a 'User Location & Demographics Report'.	Phase 2	Must
148	Back-end	Ability to report on compliance with locally agreed Service Level Agreements relating to response times to MoP messages.	Phase 1	Should
149	Front-end	Ability for force admin to generate bespoke reports with data included in the portal.	Future	Must
150	Back-end	Ability to feed data into relevant force PowerBI dashboards.	Phase 1	Should
		Auditing		

151	Front-end & Back-end	Ability to extract logging/auditing data if no in-built tool exists. One of the following is a minimum: a. Export this data into a CSV file to review in excel in a format that is workable and the auditors deem it so. b. Use of an in-built tool should one exist to complete the above. c. Clear ability to use third party tool to process this data.	Phase 1	Must
152	Front-end & Back-end	Ability to identify all users granted access to the system (including by who and when), access levels they have been granted and provision of clear pyramid of permissions so that forces can see the proposed access of users to different levels of data / permissions.	Phase 1	Must
153	Front-end & Back-end	Ability to identify specific time/dates and users for the following reasons: a. The viewing of a 'Person, Object, Location, Event' (POLE) record (or equivalent definition). b. The commencements of searches. c. The editing or creation of data within the system. d. The exporting or deletion of data within the system. e. Some navigation within the system (this is difficult to define until we are hands on).	Phase 1	Must
		Additional Use Cases		
154	Front-end & Back-end	Ability to use the tool for other use cases in future, including appointment scheduling, payments, witness/victim care and partner interactions.	Phase 2	Must
155	Front-end	The MoP will be able to register for, sign in to access/manage their portal account and receive notifications/send messages in the Welsh language.	Phase 2	Must
		Interoperability / Integrations		
156	Front-end & Back-end	Ability to interact/interoperate with respective integration platform.	Phase 1	Must
157	Front-end & Back-end	The portal will allow all existing relevant force systems to share/exchange information with the portal.	Phase 1	Must
158	Back-end	The bidder will support the development of robust and scalable force systems integrations and interfaces to facilitate seamless data exchange with iHub integration platform and Force back-end systems.	Phase 1	Must
159	Back-end	The bidder will work with iHub integration platform provider to ensure relevant NMPP API integrations can be successfully integrated into the Force system integration layer. These API integrations will adhere to modern open API standards, and best practices and patterns (where applicable). The bidder will provide clear and comprehensive API documentation and specifications for all NMPP API integrations.	Phase 1	Must
		Where APIs are not feasible, the bidder will work with the iHub Integration platform provider to ensure relevant NMPP integrations can be successfully integrated into the Force system integration layer. These NMPP integrations will adhere to the industry-standard integration	Phase 1	Must

160	Back-end	patterns and best practices. For such integrations, the bidder will provide comprehensive integration documentation, including but not limited to, schema definitions and design documentation etc.		
161	Back-end	The bidder will work with the iHub Integration platform provider to ensure all NMPP integrations are successfully implemented end-to-end across iHub integration layer and the Force back-end system.	Phase 1	Must
162	Back-end	The bidder will facilitate the mapping of data between the Force systems integration layer and iHub Integration platform, which includes API endpoints and other integrations. The bidder will provide the data mapping documentation of all NMPP integrations from the NMPP into the Force systems integration layer.	Phase 1	Must
163	Back-end	The bidder will provide data recovery capability, including the ability to re-execute NMPP data exchanges and integrations in case of errors or exceptions. This ensures that no data is lost in the event of system interruptions, errors, or other unforeseen circumstances.	Phase 1	Must
164	Back-end	The bidder will work with the iHub Integration platform provider to facilitate the generation of test data for integration testing. This will ensure all integrations are successfully tested across the NMPP solution, iHub integration platform, and Force systems integration layer.	Phase 1	Must
165	Back-end	The bidder will work with the iHub Integration platform provider to facilitate the generation of an integration testing environment that accurately replicates the production environment. This will ensure all integrations are successfully tested across the NMPP solution, iHub integration platform, and Local Force Integration layer. The bidder will support the dynamic provisioning and decommissioning of test environments as required to reduce operational costs.	Phase 1	Must
166	Back-end	The bidder will work with the iHub integration platform provider to implement relevant NMPP service-level APIs (including, but not limited to, Health Check APIs, Metrics APIS etc.) to support service management up-to the local Force systems integration interfaces.	Phase 1	Must
167	Back-end	The bidder will work with the iHub integration platform provider to implement log management APIs to support NMPP security management and troubleshooting. These APIs will support collection, aggregation, and analysis of generated logs up-to the Force systems integration interfaces.	Phase 1	Must
168	Back-end	The bidder will adhere to the NMPP standard data model for all data architecture components and integration schema definitions up to the Force system integration layer. This includes, but is not limited to, databases and data integrations through REST APIs or other industry-standard integration patterns.	Phase 1	Must
169	Back-end	The bidder will adhere to a strict change control process for all modifications to the NMPP standard data model. Any changes, including but not limited to, additions, deletions, or alterations to data structures, data types, relationships, or data definitions, must undergo a formal review and approval process before implementation. The bidder will support all stages of change control process, including but not limited to, impact assessment, risk evaluation, stakeholder consultation and approval phases.	Phase 1	Must

170	Back-end	The bidder will work with the iHub integration platform provider to develop robust and scalable integrations (e.g., REST APIs, Asynchronous APIs, batch processing etc.) that support NMPP functionalities. These integrations will support data transformation between formats (e.g., JSON, XML, CSV, etc.) used by various Force back-end systems.	Phase 1	Must
171	Back-end	The bidder will work with the iHub integration platform provider to develop integration documentation and API specifications in an agreed-upon format (e.g. OpenAPI specifications (OAS), RESTful API modelling Language (RAML) etc.) including clear descriptions of endpoints, request/response formats, and error handling. This will ensure integration documentation and API specifications are importable for documentation and knowledge management purposes.	Phase 1	Must
172	Back-end	The bidder will work with the iHub integration platform provider to develop secure APIs with Industry Standards federated authentication (e.g.: Mutual TLS, OAuth 2.0, SAML, or OpenID Connect etc.) to manage user and system authentication and authorisation.	Phase 1	Must
173	Back-end	The bidder will use JSON (JavaScript Object Notation) as the primary data exchange format for both requests and responses.	Phase 1	Must
174	Back-end	The bidder will ensure that all NMPP APIs and integrations have fault tolerance, error handling, and recovery capabilities. These capabilities include, but are not limited to, redundant hardware, load balancing, clustering, exception handling, rollback capabilities, and disaster recovery plans. The solution must ensure the system can degrade gracefully under heavy load or partial system failure without impacting the user experience.	Phase 1	Must
175	Back-end	The bidder will work with the iHub integration platform provider to implement comprehensive audit trails for all NMPP APIs and integrations. This will ensure security and compliance, as well as support troubleshooting efforts. The bidder will ensure audit trails are stored securely, with appropriate access controls to prevent unauthorised modification or deletion. The bidder will provide the ability for real-time ingestion of all audit logs into the Authority's Security Information and Event Management (SIEM) solution (Sentinel).	Phase 1	Must
176	Back-end	The bidder will work with the iHub integration platform provider to implement comprehensive logging of all NMPP integrations (such as, API requests and responses, capturing key information for auditing and monitoring purposes). The bidder will ensure logs are tamper-proof and auditable to maintain data integrity and will support the consolidation into the Authority's log management solution (Splunk) to facilitate search and filtering capabilities for efficient log analysis. The bidder will adhere to the Authority's log retention policies to manage log data volume and comply with regulatory requirements (e.g., Data Protection Act 2018).	Phase 1	Must
177	Back-end	The bidder will work with the iHub integration platform provider to implement semantic versioning on all NMPP API integrations with the iHub integration platform. The bidder will adhere to semantic versioning principles (Major.Minor.Patch). The bidder will adopt branching strategies (e.g., GitFlow) and the API version will be clearly indicated in the API documentation/request headers.	Phase 1	Must
178	Back-end	The bidder will work with the iHub integration platform provider to implement APIs to manage hierarchical access control for NMPP data, specifically utilising role-based access controls (RBAC) for granular permissions management. These role-based access control APIs will support user role management (Member of Public/Force Users/Service Support Users/National Force Reporting Users), Permission	Phase 1	Must

		management, User-role assignment and hierarchical roles management. The bidder will ensure access control mechanisms comply with relevant law enforcement standards and practices for data security and integrity.		
179	Back-end	The bidder will work with the iHub integration platform provider to implement an automated mechanism enabling real-time rollback of API updates in case of defects or unexpected behaviour in the newer version.	Phase 1	Must
180	Back-end	The bidder will work with the iHub integration platform provider to develop integration testing environment and test data that accurately replicates the production environment ensuring accurate and reliable testing.	Phase 1	Must
181	Back-end	The bidder's solution will implement robust API error handling that adheres to industry best practices and provides meaningful information for both users and system administrators (for troubleshooting).	Phase 1	Must
182	Back-end	The bidder's solution will adhere to modern API standards and principles including industry standard integration patterns and best practices to ensure security, scalability, maintainability, and ease of integration.	Phase 1	Must
183	Back-end	The bidder's solution will support all industry standard, modern API data formats for both request and response. This includes, but is not limited to: JSON (JavaScript Object Notation), XML (Extensible Markup Language) and YAML etc.	Phase 1	Must
184	Back-end	The bidder will define and implement performance benchmarks, including API response times and throughput rates. The bidder will ensure that the integration design can scale horizontally and vertically to handle increasing volumes of NMPP datasets and user activity, especially during peak periods. The bidder will consider using caching mechanisms at the API layer to optimise performance and reduce the load on backend systems.	Phase 1	Must
		Service Management		
185	Back-end	Suppliers must keep a record of actions taken against a problem or incident and make these available to force(s) upon request.	Phase 1	Must
186	Front-end	The solution will enable authorised users to easily modify content through an intuitive and user-friendly interface, without requiring specialised technical knowledge or coding skills.	Phase 1	Must

Table 5

5.3. Citizen Portal Deliverables and Timescales

5.3.1. Indicative milestones, deliverables, and estimated timescales for the delivery of Phase 1 of the Citizen Portal solution are outlined in Table 6. Final timelines and deliverables for Phase 1 will be confirmed once a supplier has been identified.

5.3.2. It should be noted that timescales for the delivery of Phase 2 of the Citizen Portal are not yet known and will be dependent on the delivery of the Phase 2 front-end requirements by Digital Public Contact.

Phase 1 Milestone	Phase 1 Deliverables	Phase 1 Approximate Timescale *(post contract award)*
Project Initiation	• Mobilisation of resources • Detailed Project Plan, including timelines.	Week 1-2
Detailed Requirements Gathering and Analysis	• Completion of user, system, and data requirements documentation	Weeks 3-5
System Design and Architecture	• High level system design specification, including technical architecture and integration plans. • System design and architecture approval.	Weeks 5-9
System Development	• Completion of core system development • Testing plans	Weeks 9-13
Testing and Quality Assurance	• Systems Integration Testing • User Acceptance Testing • Information Assurance/Security Testing • Final Acceptance Approval	Week 9-14
Deployment	• System deployment • Solution Design Document updated and handed over to appropriate Team.	Week 15
Post-Deployment Support	• On-going support post deployment • Hypercare period • Measurement and tracking of solution.	Week 16+

Table 6

5.3.3. Each milestone is to be reviewed and approved through the agreed governance channels before proceeding to the next phase. Delays or deviations from the agreed timescale tolerances will require a written exception report detailing the cause of the deviation (either predicted or actual), consequences, mitigation strategies, available options, and the required decision.

5.4. Citizen Portal User Stories

5.4.1. User Story One **(Phase 1):**

1. The MoP reports a crime to the force.

2. Crime is recorded on the Force Record Management System and assessed for investigative opportunity by the appropriate team. If it is deemed that further investigation is required, the report is allocated to the appropriate investigation team and subsequently, an investigating officer.
3. If the crime falls within the force agreed 'inclusion criteria' for a portal, the MoP receives an automated SMS/email with a link inviting them to sign up for a portal account.
4. The MoP creates a portal account, where information relating to their report(s) is accessible (including, but not limited to case status, crime reference number, crime type, date of report, and timeline of case).
5. As the investigation progresses, updates to the case on the Record Management System are assessed to deem their suitability for an 'auto-update' and if appropriate, an update is sent to the identified portal account.
6. A notification of an update is sent to the MoP, in line with their set preferences, and they sign in to check their account.
7. The MoP can see a change for their report, for example, that the status of the report is now 'allocated,' and details of their Investigating Officer are now viewable.
8. The presence of Investigating Officer details in the portal triggers the enabling of the two-way communications functionality, enabling the MoP and Investigating Officer to directly message each other and exchange text-based messages to progress the case until case closure (note that file-based messages will form part of Phase 2, detailed in User Story Three).

5.4.2. User Story Two **(Phase 1)**:

1. MoP signs in to their portal account and using the two-way communications functionality, submits a question to their investigating officer asking for an update on their case.
2. This triggers an automated task to the Investigating Officer on the Records Management System, notifying them that they have a message to respond to and automatically stamps a copy of the MoP message into the Victim Contact log.
3. The Investigating Officer replies to the MoP message.
   Note: If the Investigating Officer does not reply to the message within pre-defined timescales, an automated task is created for the Investigating Officer's Supervisor on the Record Management System to ensure the message receives a response.
4. The responding message is sent to the identified portal account and a notification of an update is received by the MoP from the Police, in line with their set preferences, and they sign in to check their account.
5. A copy of the Investigating Officer's reply to the MoP is automatically copied into the Records Management System Victim Contact log.

5.4.3. User Story Three **(Phase 2)**:

1. Investigating Officer takes a statement from the victim digitally, completing the MG11 form.
2. Investigating Officer sends a copy of completed MG11 form to the MoP (ideally directly from Athena), with an accompanying message requesting them to review for accuracy and digitally sign.
3. A copy of the Investigating Officer's message to the MoP is automatically copied into the Athena Victim Contact log.

4. The update is assessed for suitability for an 'auto-update' and if suitable, it is sent to the identified portal account.
5. A notification of an update is received by the MoP from the Police, in line with their set preferences, and they sign in to check their account.
6. The MoP can see a new message for that report and, in this example, that the Investigating Officer has sent them a message with a document attachment for their review and signature.
7. The MoP reviews the MG11 and deems it to be accurate. MoP digitally signs the document and using the two-way communications functionality, sends a message to the Investigating Officer, attaching the signed MG11 form.
8. This triggers an automated task to the Investigating Officer on Athena, notifying them that they have a message to respond to.
9. A copy of the MoP responding message automatically stamps into the Victim Contact log (including date/time) and a copy of the signed MG11 is automatically uploaded to the Athena Investigation so as the Investigating Officer can determine whether it will form part of the case.

5.5. Citizen Portal Aftersales Support

5.5.1. Indicative response and target resolution times are outlined in Table 7.

- Support will be available for critical and high priority incidents 24/7 via telephone support number and a support portal.
- Support will be available for medium and low priority incidents between 8am-5pm on UK working days via a support number, email, and/or a support portal.

Priority	Response Time	Target Resolution	Description
Critical	15 Minutes	Within 4 hours	Serious issue – business is not able to function.
High	2 Hours	Within 1 Working Day	Significant impact but business is able to function.
Medium	1 Working Day	Within 3 Working Days	Small impact to the business but issue can be circumvented.
Low	3 Working Days	Within 10 Working Days	Negligible impact to the business.

Table 7

- Change Management process to be provided and forces to be notified in advance of any regular maintenance, including expected downtime and testing conducted to minimise disruption to users and enable forward planning where required. The supplier should also notify forces of emergency change with as much notice as possible to enable impacts on business provisions to be established.
- Problem Management process to be provided with expected timescales for development and release of defect fix patches (for example quarterly).
- The supplier must detail their hardware replacement programme and any impact on project delivery.
- Monthly reporting and service review meetings.
- Service Level Agreement detailing the support process. This will be reviewed by forces prior to contractual agreement to ensure it includes a breakdown of service level agreements, support phone

number, email address and portal links, escalation details and penalties if service level agreements are not met.

- Forces should also have the option to opt for a 'managed service' and suppliers should provide pricing structures around the cost for a 'managed service' and any continual service improvement.

6. LOT 3: Customer Relationship Management

6.1. Customer Relationship Management Scope

6.1.1. Currently, forces record Crimes and Incidents in the respective Storm and Athena systems but require a system for recording all interactions with the public, including those that fall outside of those systems. It is anticipated that the CAD and RMS systems would remain, with a CRM being used as an overlay.

6.1.2. Forces also require a single "view of the truth" when researching systems that hold relevant information on a member of the public – currently multiple systems are manually searched, and a CRM would allow for that information to be presented on a single screen to allow the operator to quickly and easily digest relevant information about the contact.

6.1.3. A two-way, read/write integration would be needed between the CRM and source systems to maintain this single version of the truth.

6.1.4. Forces would also like to utilise advancing technology in the form of AI or Bots to support the human operators to improve efficiencies.

6.1.5. Supported LiveChat using Chat bot and voice bot – Forces would like the ability to offer fully or partially scripted chat bot responses and to work with Contact Operators to offer recommended answers and integrate with AI.

6.1.6. Incoming contact need to shift from mainly telephony to digital means – omnichannel queue management would be needed to support non-emergency contact via digital channels such as social media, 101 calls and LiveChat.

6.1.7. Forces need the ability to shift the member of public from the receiving channel over to the most appropriate one for both the member of public and for the force. Currently there is limited ability to do that, forcing the contact to remain on the same channel, regardless of whether it is the most appropriate one.

6.1.8. An integrated platform as a service would offer simpler system integration when compared to point to point connections. System integrations should be direct with source systems instead of utilising a data warehouse.

6.1.9. Call data for forces is available in the appendix to support responses on CRM.

6.2. Customer Relationship Management Detailed Functional Requirements

6.2.1. The functional requirements for a Customer Relationship Management solution are outlined in Table 8.

ID	Description – Business Functional Requirement	Priority
1	Ability to change brand (e.g. logo and colours).	Must
2	Available 24/7, 365 days a year.	Must
3	Comply with the latest Web Content Accessibility Guidelines (WCAG), currently version 2.2.	Must
4	Comply with force policies relating to the Review, Retention and Deletion of information to comply with the PIRM code.	Must
5	Where the service will be used across multiple forces, we need access to data to be restricted on a force per force basis but also be able to share data between forces where appropriate.	Must
6	The use of advanced IVR on our telephony lines (including voice recognition) to replace our traditional IVR options, to better understand callers' reason for calling and to apply appropriate messaging, prioritisation, routing and queue management.	Must
7	The use of Live Chat/ChatBot to manage non-emergency contact, this includes providing relevant and accurate auto-responses and to apply appropriate messaging, prioritisation, routing and queue management.	Must
8	Multi-channel management – allowing us to manage all demand across all our channels, including telephony, website, live chat and social media. This includes flexibility to move demand from one channel to another (e.g. if emergency related), prioritise demand (e.g. based upon key words) and adjust the operating model based upon resource availability and other KPIs.	Must
9	Ability to feed live time queues across all channels to wall boards.	Must
10	A single interface providing a staff member/Officer with a single view of information from multiple systems. This must include previous contact (within all channels) and be presented in chronological order.	Must
11	The system will present automatic summaries of information to Contact Management Colleagues based on information from core systems for a given contact.	Must
12	Ability for any updates on information made at the single interface to be written back to the source system to ensure one version of the truth.	Must
13	All contacts and outcomes to be recorded to identify non-value/failure demand, irrespective of whether a CAD or RMS record is created as a result	Must
14	The system will identify where there is differing information stored on core systems that relate to the same MoP for action or reporting.	Must
15	Ability to verify details of persons making contact using an automated method of authentication.	Must
16	Ability to send/record communications with members of the public through different contact means – included but not limited to email and SMS.	Must

17	Ability to rate the contact in terms of wellbeing/impact and system to automatically assign a THRIVE (Threat, Harm, Risk, Investigation, Vulnerability, Engagement) / THRIVE+ (Threat, Harm, Risk, Investigation, Vulnerability, Engagement, Prevention) based on content.	Should
18	Ability to present staff with pre-agreed scripts and questions to ask the contact.	Must
19	Ability to auto-tag contacts based on answers provided to the pre-agreed scripts/questions.	Must
20	Auto-filling of standard forms using AI (e.g. safe-guarding referrals).	Must
21	Ability to use pre-set templates (e.g. email/letter/SMS) for standard outgoing communications	Must
22	Ability to transcribe calls/audio/media.	Must
23	Ability to support quality assurance processes for calls/contacts to assess interactions, removing reliance on manual dip sampling.	Must
24	Allow authorised force users to access portal information under relevant system access management and control procedures.	Must
25	Integration with HR system to support automatic provision of appropriate access to CRM system.	Should
26	A full suite of Management Information that is readily available for the appropriate users to perform proactive reporting. Data must be easily readable for the appropriate users.	Must
27	Ability to feed data into relevant force PowerBI dashboards.	Should
28	The solution will enable authorised users to easily modify content through an intuitive and user-friendly interface, without requiring specialised technical knowledge or coding skills.	Must
29	The system will enable users to log in to the system with one set of details (e.g., Single Sign On).	Must
30	Ability to create standard and bespoke reports.	Must
31	Ability to transfer contacts internally/externally via the system (e.g., Contact Operator to Rapid Video Response team).	Must
32	Connection to Gazetteer to support address matching.	Must
33	Suppliers must keep a record of actions taken against a problem or incident and make these available to force(s) upon request.	Must
34	Any live chat provision needs to be able to be launched from force's local Single Online Home pages.	Must
35	Ability to integrate to force dynamic duties management systems.	Should

Table 8

6.3. Customer Relationship Management Deliverables and Timescales

6.3.1. Indicative milestones, deliverables, and estimated timescales for the delivery of a Customer Relationship Management solution are outlined in Table 9. Final timelines and deliverables will be confirmed once a supplier has been identified.

Milestone	Deliverables	Approximate Timescale *(post contract award)*
Project Initiation	• Mobilisation of Resources • Detailed Project Plan including timelines.	Week 1-2
Detailed Requirements Gathering and Analysis	• Completion of user, system, and data requirements documentation	Week 3-15
System Design and Architecture	• High level system design specification, including technical architecture and integration plans. • System design and architecture approval	Week 16-20
System Development	• Completion of core system development • Testing plans	Week 21-26
Testing and Quality Assurance	• Systems Integration Testing • User Acceptance Testing • Information Assurance/Security Testing • Final Acceptance Approval	Week 27-31
Deployment	• System Deployment • Solution Design Document updated and handed over to appropriate team.	Week 32
Post-Deployment Support	• Ongoing support post deployment • Hypercare period • Measurement and tracking of solution.	Week 32+

Table 9

6.3.2. Each milestone is to be reviewed and approved through the agreed governance channels before proceeding to the next phase. Delays or deviations from the agreed timescale tolerances will require a written exception report detailing the cause of the deviation (either predicted or actual), consequences, mitigation strategies, available options, and the required decision.

6.4. Customer Relationship Management User Stories

6.4.1. User Story One**:**

1. Contact Operator receives a 999 or 101 call and is presented with any previously known information about the caller based on name or caller number including but not limited to name, contact details, Threat, Harm, Risk score, preferred method of contact and summary details of previous contacts.
2. Contact Operator/Dispatcher is shown relevant information around risks to officers, and information useful to dispatch.
3. Contact Operator/Dispatcher is shown relevant information from system interfaces such the Police National Computer (PNC), firearms information, Athena record.

4. Contact Operator adds information to the CRM system which then updates the source system via a two-way read/write interface.
5. Contact Operator has the call transcribed into a log by AI and this is posted back to desired integrated software, for example STORM, Athena or the Police National Computer.
6. Contact Operator is able to review incoming channels including but not limited to calls, social media, live chat, emails and the system to prioritise incoming contact which is then presented to the Contact Operator.
7. A MoP chooses to live chat to the Force via the force website hosted on Single Online Home.
8. MoP selects to live chat with the force, and is firstly responded to by AI, which notifies the MoP that they are talking to a Bot. The Bot provides an answer and signposts the MoP to the correct resources including the Force website if appropriate.
9. MoP selects to live chat with the Force, and is firstly responded to by AI, which notifies the MoP that they are talking to a Bot. The Bot cannot answer the query and transfers the MoP to a relevant Contact Operator.
10. AI provides suitable responses to a chat query and the Contact Operator selects whether reply is suitable or overwrites an alternative response.
11. MoP selects to live chat with the force, and is firstly responded to by AI, which notifies the MoP that they are talking to a Bot. The AI recognises a key word in the chat, or answers to a series of questions, and directs the MoP straight to a Contact Operator.
12. Contact Operator uses a copy of call scripts in the CRM to lead the MoP through a set of questions to gain information on specific call types.
13. MoP has included a typo in their details and the CRM highlights any errors or discrepancies to the Contact Operator.
14. MoP can be sent information or survey following the call by various contact means such as text message, email, via the portal etc.
15. Member of staff uses the CRM to see information data about a message, such as when it arrived, when it was read and by whom.
16. A member of the Support Team obtains user metrics and statistics based on system usage and uses them for analysis, including appropriate dashboards.
17. Data exports to Power BI to allow the Force Analysts to complete trend analysis.

6.5. Customer Relationship Management Aftersales Support

6.5.1. Indicative response and target resolution times are outlined in Table 10.

- Support to be available 24/7 via a telephone support number and/or a support portal, as CRM is considered a critical function. Indicative response and target resolution times are outlined in Table 10.

Priority	Response Time	Target Resolution	Description
Critical	15 Minutes	Within 4 hours	Serious issue – business is not able to function.
High	2 Hours	Within 8 hours	Significant impact but business is able to function.
Medium	1 Working Day	Within 3 Working Days	

			Small impact to the business but issue can be circumvented.
Low	3 Working Days	Within 10 Working Days	Negligible impact to the business.

Table 10

- Change Management process to be provided and forces to be notified in advance of any regular maintenance, including expected downtime and testing conducted to minimise disruption to users and enable forward planning where required. The supplier should also notify forces of emergency change with as much notice as possible to enable impacts on business provisions to be established.
- Problem Management process to be provided with expected timescales for development and release of defect fix patches (for example quarterly).
- The supplier must detail their hardware replacement programme and any impact on project delivery.
- Monthly reporting and service review meetings.
- Service Level Agreement detailing the support process. This will be reviewed by forces prior to contractual agreement to ensure it includes a breakdown of service level agreements, support phone number, email address and portal links, escalation details and penalties if service level agreements are not met.
- Forces should also have the option to opt for a 'managed service' and suppliers should provide pricing structures around the cost for a 'managed service' and any continual service improvement.

7. Appendix

<table>
<tr><td>1</td><td>Example User Journey</td><td>Example User Journey.pdf</td></tr>
<tr><td>2</td><td>Force Call Data
<table>
<tr><th>2024 call volumes</th><th>Emergency (999)</th><th>Non-emergency (101)</th><th>Total</th></tr>
<tr><td>Bedfordshire</td><td>120,272</td><td>161,719</td><td>281,991</td></tr>
<tr><td>Cambridgeshire</td><td>145,834</td><td>234,982</td><td>380,816</td></tr>
<tr><td>Essex</td><td>310,007</td><td>706,767</td><td>1,016,774</td></tr>
<tr><td>Hertfordshire</td><td>179,583</td><td>272,899</td><td>452,482</td></tr>
<tr><td>Kent</td><td>324,973</td><td>580,338</td><td>905,311</td></tr>
<tr><td>Norfolk</td><td>126,062</td><td>284,563</td><td>410,625</td></tr>
<tr><td>Suffolk</td><td>107,871</td><td>237,013</td><td>344,884</td></tr>
</table>
</td><td></td></tr>
</table>