**Specification for Social Media Platform**

The Commissioner is acting as the lead for this Contract and the Contractor acknowledges and accepts that the Contract is available to the following parties as Other Contracting Bodies:

* Police and Crime Commissioner for Gwent

Each Other Contracting Body shall enter into a separate contract with the Contractor in relation to that Commissioner’s own requirements. The Contract shall be divided into two Lots by police force area as detailed below:

* Lot 1 – Dyfed Powys Police
* Lot 2 – Gwent Police

**Introduction**

Social Media is increasingly the primary tool used by members of the public to engage with the Police. With a wide array of options for engaging and increasing numbers of Force social media accounts in use, it is vital that the Force mitigates this significant reputational risk through the acquisition of an appropriate social media management platform, which affords content control and monitoring control over the Force’s social media presence.

**Dyfed Powys Police**

Dyfed Powys Police’s current social media estate is across four main social media channels. Currently, all access to social media across Facebook, Twitter, and Instagram is ‘native’ – meaning that the channels are directly accessed by staff. The Force Digital Communications Strategy has been developed in line with the work of the NPCC Social Media Project, its Target Operating Model and Digital Estate Guidance for social media in policing, and identifies the need for streamlining of our social media presence. We will undertake a significant reduction in the total number of ‘official accounts’, bringing benefits to the organisation in making our voice clearer, and to public accessibility of information. This is particularly important given legislative changes due in December 2020, which will bring a requirement for monitoring of our official channels.

Dyfed Powys Police require their contract to be in place and invoiced prior to 31/03.2020.

**Gwent Police**

In 2017 it was recognised that social media was growing as a primary tool used by members of the public to engage with the Police. In order to mitigate against the risk of an inability to engage in this manner the force identified that it was necessary to acquire a social media management platform, which afforded content control and monitoring control over the Forces social media presence. As a result and following the successful submission of a Business Case the force purchased its first social media platform tool.

At this time the force adopted the use of licenses for 200 users across the force. Primary users are based within the corporate communications team and the force control room. Users currently provide outbound information and reply to inbound information. Since its inception the value of the tool has become clear with an emphasis on identifying future developments of the platform, reporting and auditing tools and administrator controls being paramount.

Following a national review it was clear that Gwent needed to review and potentially upgrade its current provision and hence has contributed to the development of this process.

Gwent’s current contract is due to expire 30/09/2020.

**Technical Requirement**

1. **Security and Data Protection**

1.1 The Social Media Management Platform will operate on both force mobile, laptop and desktop environments which conform to sector specific standards. The detail is available from the Police ICT Company, details can be found here: <https://ict.police.uk/national-standards/security/>.

1.2 All data must be held in the UK on a secure server/cloud.

1.3 The solution provider must confirm if the tenancy is Private, Community, Public or Hybrid.

1.4 The provider must provide evidence that they achieve the 14 National Cyber Security Centre Cloud Security Principles (specific details available on request).

1.5 The provider should have and evidence Cyber Essentials accreditation.

1.6 The provider must be able to evidence that IT Health Checks are conducted by testers with industry recognised qualifications. (CHECK, CREST or Tiger schemes). They should also allow the force to review the result of any IT Health Check highlighting what remedial work was required and evidence to show the work has been completed or is in progress.

1.7 The provider must be able to evidence what ISO accreditation any cloud solution has achieved (e.g. ISO 27001:2015, ISO27017:15, ISO 27018:2015), and provide copies of ISO certificates.

1.8 The provider must be able to provide any other relevant technical information as part of IT security assurance.

1.9 A Data Processing Contract must be implemented prior to system go-live. It must be noted and agreed within the Data Processing Contract that all personal data belongs to the force including performance data.

1.10 The technical solution must be programmable to ‘weed’ or delete information that should not be retained in line with MOPI guidance. It would be desirable for a user to be able to select which MOPI group the information was categorised in to enable the user to select the appropriate group when triaging a post or message.

1.11 Social media platform provider staff will not be able to access the personal information held on behalf of the force or user except in a full audited process as required by other requirements in this document. Any social media platform staff required to access such personal information must agree to be vetted in line with required standards.

1.12 There must be an ability for internal users to be suspended from access but not fully deleted from the system to ensure integrity of records and audit processes. As a minimum standard any deletion from the system must not affect the audit trail of previous actions by that specific user. Suspended users should not count towards any licensing cost.

1.13 The platform will provide, by exception, support for a valid request for the ‘right for erasure’ aka ‘right to be forgotten’ – details available from the ICO <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-thegeneral-data-protection-regulation-gdpr/individual-rights/right-to-erasure/>.

1.14 The platform must provide details of the security scanning that will be provided on the inbound content

1. **Social Media Channel Integration**

2.1 The social media management platform must integrate fully with the main social media channels used by the force as a minimum standard – including Facebook, Twitter and Instagram.

2.2 It must be able to monitor simultaneously inbound and outbound content from a number of different social media platforms in one place, potentially from a number of different accounts

2.3 The platform must have an identified progressive plan in place for being able to take feeds from different social media tools

2.4 The platform must provide access to all features of these channels.

2.5 The platform must provide access to the features of Facebook Groups, and allow users to publish content to these groups as a Facebook Page.

2.6 The platform must also integrate fully with the direct/private messaging functions of each channel.

The platform must support the integration of

Dyfed Powys Police: 18 Facebook Groups; 38 Facebook Pages (to feed the groups), 45 Twitter accounts and 1 Instagram account as a minimum, with scope to increase this if required.

320 user licences are required.

Gwent Police: 2 Facebook Pages, 25 Twitter accounts, with scope to increase this if required.

74 user licences are required.

1. **User Interface – Desktop**

*3.1 User/Role specific interface*

3.1.1 Users of the social media management platform should have a customisable view, which is based on their permissions and role.

3.1.2 The platform should support the sharing of well-designed role specific views across teams.

3.1.3 Functionality not required for the user’s role (based on permissions) should not be shown, the screen will render as a suitable format.

3.1.4 The user interface must be intuitive to use, help available and designed to support the browsers available across police technology (including Internet Explorer, Microsoft Edge and Google Chrome).

3.1.5 Administrators must have the ability to create and edit user accounts and to remove access if required with immediate effect. They must also have the access for delegating different permissions dependent on the role and the responsibility of the individual.

*3.2. Workflow*

3.2.1 The management platform must provide a way to hand off information to different users/teams and there should be an auditable log of who reviewed the post/message and when the post was actioned.

3.2.2 The administrators within the force must be able to manage and design workflows, teams and search terms.

3.2.3 There will be a requirement to demonstrate the documented decision tree behind any automatic processing.

3.2.4 The management platform must have the capability to be programmed with keywords. If a post or message with a keyword is received this should notify a user which should be specified by each keyword.

3.2.5 The user/workgroups should be notified via a range of notifications specified by the administrator and/or user through the platform.

*3.3. Tagging / Categorisation*

3.3.1 The management platform must allow for the effective management of tags or categorisation of content, this tagging will assist in the reporting, analysis and management of content.

3.3.2 Both inbound and outbound content must be able to be tagged/categorised.

3.3.3 The ability to tag or categorise outbound content should be able to take place both on initial publication/creation, and retrospectively.

3.3.4 The force must be able control and define the tags and rules for use, this function should be limited to administrators.

*3.4. Realtime updating*

3.4.1 The platform must ‘pull in’ posts, comments, reactions and direct messages in ‘real time’. There should be no delays in messages being received due to the use of the management platform.

3.4.2 Similarly, the lag between a colleague posting or replying in real-time must feel as close to instant as practical and the user experience for both the citizen and police user should feel seamless. This includes the private messaging side of platforms, eg. Facebook Messenger

*3.5 Publishing & Replying*

3.5.1 The platform must enable all users to publish posts to social media networks, both publicly and in private messaging functions.

3.5.2 The management platform should have the additional functionality for posts to be approved before being published on the social sites, which can be switched on or off as appropriate.

3.5.3 All users must be able to complete actions on all posts or messages through the platform as they would on native sites.

3.5.4 The platform must provide a unified cross-channel inbox of inbound content aligned with the workflow requirements at 3.2.

3.5.5 Within the platform any user must have access to the previous interactions held within the social media management tool only. This will include access to tags, notes and previous inbox actions and replies.

3.5.6 The platform must have the ability to both publish and receive images and video. The platform must have the ability to allow images and video to be both posted through it and as a minimum images to be received from external sources.

*3.6 Content library*

3.6.1 The platform must have the capability to store stock images that can be easily searched and categorised either by campaign or department.

3.6.2 Users will be required to categorise content at point of upload and the force will require the ability to apply governance rules to uploads (eg expiry date).

3.6.3 Where an expiry date is set for an asset the product will automatically withdraw from use.

3.6.4 Administrators must have the ability to revoke access to assets immediately.

3.6.5 The revocation of access to assets by administrators should also highlight if any scheduled posts need to be reviewed which may be using the asset.

3.6.6 The library should maintain a record of the use of the asset for review by administrators.

3.6.7 The content library should manage formatting of content to the specific requirements of each social media channel.

3.6.8 The content library should manage formatting (particularly for video/audio) to ensure the content is natively available within the social media channel.

*3.7 Content scheduler*

3.7.1 There must be a content scheduler built into the platform.

3.7.2 There must be a visual / calendar view of both planned and previously posted content.

3.7.3 Scheduled content should be easily able to be moved within the calendar view, or copied to a different date.

3.7.4 The platform should support multiple scheduling times within the same window.

*3.8 Take-over button*

3.8.1 In times of critical incidents, the software must have the capability to allow an admin or super-user account to take control of all accounts and stop any prescheduled posts from going out without authorisation from the team managing the response to the incident.

*3.9 Social media monitoring*

3.9.1 The management platform must be easily configurable, to add or remove accounts to be monitored.

3.9.2 The platform must have the ability to monitor inbound and outbound content from a number of different social media channels in one dashboard, from a number of different accounts linked by the force.

3.9.3 The desktop user must have the ability to view a range of streams based on user/group highly customisable Boolean logic queries across several channels.

3.9.4 Identified content must be easily shared outside of the management platform to other departments when necessary.

3.9.5 This action must also be recorded within the audit (to the point the issue is exported outside the platform).

3.9.6 The monitoring function must fully integrate into the tagging protocol established by the administrators.

*3.10 User or Group Messaging – internal*

3.10.1 The platform must allow internal users to make and share notes and tags on interactions securely with individual users or teams. This will also be fully auditable.

3.10.2 The users must have access to a library of useful and pre-approved content, templates, and stock responses.

3.10.3 During lock down / critical incidents the ability for a customisable message to be displayed immediately after login should be available.

*3.11 Image editor*

3.11.1 The platform must allow users to reformat, edit or correct images including the functionality to mask faces, registration numbers or specific detail when required by the force’s internal standards and policies. The final image published on social media channels will be a flat image and not include any of the hidden detail which an advanced photo editor could retrieve.

3.11.2 The platform will quickly enable images published to include a watermark set by administrators.

* + 1. The image editor must include access to a mobile devices’ camera function.

3.11.4 All images must be published to the best standard format for the channel being published to.

*3.12 Spelling/grammar check*

3.12.1 All written content should automatically be checked against a UK English spelling and grammar check.

3.12.2 The administrators should be the only users able to customise the spelling dictionary, this will mainly be used for the sometimes-unusual spelling of locations.

3.12.3 The platform should support communication in Welsh. The product should recognise the Welsh language and provide a Welsh dictionary when the operator is working in Welsh.

*3.13 Content Publisher Function*

3.13.1 The functions available to the user must be defined by the user’s specific permissions and settings.

3.13.2 Users must have the capability to create top-level content, but if posting to different channels customise the specific post for each channel based on the properties of that channel. The platform will assist with information on character limits and other functionality.

3.13.3 Users must be able to preview how the content created would look specifically on each platform before confirming publication

3.13.4 The user must have immediate access to the scheduling functions whenever posting.

3.13.5 The user should be alerted if posting content on a channel when other content is already scheduled.

3.13.6 Users should be able to target content based on the native functionality of the channel, i.e. where Facebook allows users to target content based on location, gender or interests etc then the platform provides this interface.

*3.14 Link management*

3.14.1 The platform should provide an in-built link shortener, and must ensure a seamless user experience allowing the user to simply paste or type a link, which is then automatically shortened prior to publication.

*3.15 Additional Features*

3.15.1 The platform should have an in built automatic profanity filter for inbound comments (where applicable to the channel), which is customisable by administrators.

3.15.2 The platform should provide a warning of profanity before publishing should it appear in the text of outbound content.

3.15.3 The platform must allowing hiding of comments or content by administrators, or keyword filters to automatically complete this process.

1. **User Interface – Mobile**

*4.1 Technical Environment*

4.1.1 The management platform must provide a mobile application to the host forces (and later national emergency services network ESN) for deployment to work owned/managed devices (Android) via a device management platform.

Dyfed Powys Police currently utilises Blackberry MDM

Gwent police currently utilises Airwatch with Samnox Security

Under the National Enablers Program Office 365 deployment may utilise Microsoft In Tune; all platforms must be supported.

4.1.2 Full functionality and technical support must be provided to ensure security compliance as devices work within a secure space.

4.1.3 The data usage requirements of the mobile application should not be excessive, and size of uploads limited to suit a 3G/4G environment.

4.1.4 The system should be compatible with integration to Microsoft Active Directory allowing single sign-on for all users.

4.1.5 The system should have Role Based Access Control (RBAC) configurable by the force.

*4.2 User Interface*

4.2.1 The management platform must provide a truly mobile experience in-line with the modern standards experienced on more domestic tools. The user will not require a stylus or other hardware interface to interact with the functions on the mobile platform.

4.2.2 The management platform should provide a ‘single click’ way to hand off information to different users/teams and there should be an auditable log of who reviewed the post/message and when the post was actioned as part of the workstream requirement highlighted above.

*4.3 Publishing/Replying*

4.3.1 The mobile version of the platform must allow for monitoring of the live feeds from social media channels as native access would.

4.3.2 The mobile version must allow instant publishing to the channels, including publishing multimedia content, and must fully integrate with Facebook Groups.

*4.4 Content Interface*

4.4.1 The mobile version of the content interface should maintain the properties of the desktop interface but be a truly mobile experience.

*4.5 Content scheduler*

4.5.1 Mobile users should be able to see a limited (date range) view of content planned for publication based on their user permissions.

4.5.2 Similarly, mobile users should be able to use the scheduling functions when using the mobile publication tool.

*4.6 Take-over button*

4.6.1 Mobile users should be able to see that a take-over has been activated.

*4.7 Social Media Monitoring*

4.7.1 The mobile user must have a mobile view of their personal inbox (based on the access of the user) which enables the basic functionality below:

Mark as read / reply / take to private / pass to workflow / like / share / add notes / allocate to other user/workgroup / amend sentiment.

4.7.2 The mobile user should have a limited view of social listening tools highlighted within the desktop requirements.

4.7.3 The mobile user should be able to conduct basic open source searches within the management platform.

*4.8 Mobile Dashboards*

4.8.1 The mobile user must have a basic dashboard to provide an overview of current demand/actions allocated to them.

4.8.2 Navigation of the dashboard should be clear and simple.

1. **Audit Capabilities**

*5.1 Audit Log*

5.1.1 The platform must date and time stamp with individual users details when they have taken any action on a post including - opening, responding, resolving, assigning to another team, editing (including version keeping), deleting (unpublishing as all content will need to be retained).

5.1.2 The administrators or other selected users must be easily able to export a complete timeline for both sides of a conversation which include all the above actions in a secure tamper evident format what could be presented as evidence in criminal, civil or coronal proceedings. A tamper proof/evident record will be maintained in the social media platform which would allow demonstrated the validity of such reports.

5.1.3 The platform must be able to provide to courts (if required) evidence of access to data by user both within the force and the social media platform.

*5.2 Captured at first contact*

5.2.1 All messages and posts that have been received must be captured within the platform even if the post or message is deleted by the user on the native platform.

5.2.2 This should be possible to export on demand with a simple user interface providing tamper proof / evidence reports for integration into other systems.

5.2.3 The social media management platform provider must provide evidential statements explaining the process for capturing and securing the reports if required by court. On rare occasions senior technical or management representatives may be required to attend court or meetings with legal advocates to provide reassurance and detail on the detail of how reports are recorded and logged by the system.

*5.3 Metadata*

5.3.1 The metadata associated with each interaction should be retained by the management platform. This will prevent the need to contact the social media platforms themselves should metadata be required for evidential purposes.

1. **Performance Monitoring**

*6.1 Analytics*

6.1.1 The platform must provide full background analytics to enable effective performance monitoring. This should include outgoing content performance to measure effectiveness of social media activity.

6.1.2 The timespan of reports must be user definable.

6.1.3 Automatic report generation to a user defined schedule should be supported.

6.1.4 Reports will be provided in several formats but must include Excel/CSV support, PDF and charts provided in a usable format for transfer into Office 365 products.

6.1.5 The platform must provide keyword, tag or category-based reports

6.1.6 User and team-based reporting should be supported.

6.1.7 User activity reports should be available highlighting last log in detail by user which can be filtered to defined timescales.

6.1.8 The management platform should retain insights/analytic data for deleted posts, or will continue to include these in higher level statistics.

6.1.9 The platform should either provide a live time demand feed for supervisor management or monitoring or be able to interface with systems that currently can.

1. **Business continuity**

*7.1 Changes to Social Media Platforms*

7.1.1 The social media management tool provider must ensure that they have a clear plan on development seeking to enable connections to new channels, and keep up to date with any changes made by already enabled social media channels to API’s/code should the need arise.

7.1.2 The social media management provider must alert force level admins of the impact of future and immediate changes from the channels immediately and provide timelines on updates that affect the user experience.

7.1.3 The management platform must be web based, allowing access from anywhere for business continuity purposes.

*7.2 ‘Always On’ Service*

7.2.1 The social media platform must maintain a business continuity plan to ensure the highest industry standards. This will include 24/7 central support to ensure platform resilience, integrity and security (rather than user support).

7.2.2 The provider must provide a help desk function and have an agreed service level agreement (SLA) in place which aligns to the organisations Business Continuity Management plan of 4 hrs for a response. The help desk provisions should be available for a minimum of during office hours but there must be an out of office provision to report total failures of services and an ability to achieve the SLA out of hours.

7.2.3 A Gold, Silver and Bronze SLA should be set which as a minimum must include a Gold response of being able to receive incoming and outgoing direct private messages at a fix of 4 hours.

7.2.4 The platform must be recognised by the provider as an emergency contact system and faults/downtime will be rectified urgently.

7.2.5 The force admins must have an escalation route when issues are identified.

7.2.6 Force admins must be alerted prior to planned outages.

7.2.7 Planned outages should take place at times of lowest demand.

*7.3 Integration*

7.3.1 The solution should allow integration in to existing and future force call management solutions allowing demand across all platforms to be monitored, resources to be flexed to deal with the demand in order to provide and effective and efficient service.

DPP’s contact centre legacy solution comprises of Cisco Unified Contact Center Enterprise (UCCE)  version 8.5 supported by Cisco Unified Communications Manager (Call Manager - CUCM)  version 8, however work is underway to upgrade these to UCCE version 11.6 with CUCM version 12.

Gwent contact centre solution is Open Scape managed by ATOS which is used in the FCR to route 101 and 999 calls

1. **User Management**

8.1 The platform must provide an easy to manage, clear and simple interface for administrators to manage user access.

8.2 Within this interface, allocating access to different social media channels, and user membership of teams must be a simple process and must be limited to administrators.

8.3 Either a strong standard password policy, or a customisable one set by the force must be in place.

8.4 Creation, editing and suspension of user accounts must be instant.

1. **Training**

9.1 A train the trainer package must be available and provided to at least four members of staff at the time of initial procurement.

9.2 Should upgrades be made to the product by the provider, new facilities bought on line or changes made additional support should be provided in order to ensure the organisations effective and accurate use of the product. On-line guides or guide documents should be available for reference.

9.3 Within the train the trainer, package particular emphasis should be placed on analysing the effectiveness of a campaign or social media interaction to understand and use the analytics appropriately.