WhatsApp Business Approval Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police, Fire and Crime Commissioner are required to adhere.

Procedure Statement

WhatsApp Business is a freeware and cross-platform messaging and Voice over Internal Protocol (VoIP) service owned by Facebook. The application allows the sending of instant messages, making voice and video calls, and the sharing of media such as images or videos, documents, and user location with other WhatsApp users, both individually and in groups. The use of WhatsApp is via an internet connection. WhatsApp Businesses allows organisations to create several accounts under different business mobile numbers and customise their profile description to allow audiences to communicate with them.

Overarching Policies:

Force Information Security Policy

Procedures:

Social Media and Community Messaging Procedure

Security Incident Reporting Procedure

Internet and E-mail Procedure

Other Documents:

Appendix A - Terms of Usage for WhatsApp Business
Appendix B - WhatsApp Business audit scope
Appendix C - Privacy statements for WhatsApp
Appendix D - Case Study of Helmsley Mobile Rural Watch
Appendix E - IAO Decision Making Tree
Appendix F - WhatsApp Business approval process
Appendix G - WhatsApp Business detailed guidance
Appendix H - WhatsApp Set up instructions

Process

The use of WhatsApp requires NYP to instil great trust in the end users and therefore only selected networks should be authorised to enable NYP to benefit from the value of the engagement whilst balancing any risks associated with using the application.

Decisions to use WhatsApp should be made by IAOs on case by case basis, and wherever possible, alternative means of communication that achieve the same goal should be favoured. Where no alternatives are available, the IAO should ensure that the rationale behind the use of the application and the governance of its use are recorded and auditable. The use of the application should not be authorised unless it significantly contributes to achieving the intended purpose. Therefore, WhatsApp should not be considered suitable for general use.

It is crucial that NYP, and specifically IAOs authorising the use of the application, remain conscious of the level of sensitive data sent via the platform. The terms of usage **(Appendix A)** stipulate that under no circumstances should sensitive information, media or links be shared. The information shared by NYP via the platform and the language used when communicating via the platform ought to align with the way information is shared similarly on Facebook, Twitter, Instagram, the community alerting system and the information shared publicly by more traditional means.

To obtain approval for WhatsApp Business use, the IAO should be approached by the business lead wanting to use the platform with some rationale and initial considerations around risk and mitigation already having been made. The IAO and business lead should then document any identified and mitigated risks and manage them through the usual risk management processes. If it is advised that the user case can be approved, the business lead (requestor) or Information Asset Owner will complete the relevant e-form to alert the ISO of the user case which, once reviewed by the ISO, will trigger an ICT workflow to grant named users access to WhatsApp Business.

NYP's corporate stance is that we should be risk conscious, rather than risk averse. Being risk conscious means being aware of risk and taking balanced decisions about how much of a risk we really face, and whether it can be managed or mitigated. Therefore, the Force's Risk Matrix should be used to assist with the risk-based decision-making. More information on this can be found on the Risk and Assurance subsite or within the detailed guidance available at **Appendix G**.

Details of the approval process are available at **Appendix F**.

As per the detailed approval guidance available at **Appendix G**, this procedure will enable:

- The collection of sufficient information about a process/initiative/operation to allow a decision to be made as to whether the use of WhatsApp Business could significantly contribute to achieving the intended purpose;
- Any privacy, security or information governance risks to be identified, documented and considered, and effective, proportionate controls to be put in place;

The guidance also discusses the key risks which the IAOs bear in mind when considering WhatsApp Business use:

- Data could be retained for excessive periods of time and in contravention of the Data Protection Act 2018;
- Data could be processed outside of the UK which could mean data would be transferred without the necessary agreements in place to safeguard the information in transit and when at rest, but also that it could be subject to the receiving country's laws which may compromise the confidentiality of the data;
- NYP and the PFCC could fall victim to a security breach from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, police data transmitted, stored or otherwise processed through WhatsApp Business;
- The remote probability that NYP and the PFCC departments utilising the application may not implement sufficient mechanisms to meet disclosure obligations under Criminal Procedure and Investigations Act 1996, or the legislative data protection obligations to ensure that individual's information rights such as right of access and the right to rectification and erasure are upheld; and
- The risk of WhatsApp Business to be used outside of the agreed scope, or for Officers, staff or members of the public to exhibit inappropriate and/or unethical behaviour.

The IAO should make a risk- based decision keeping in mind the known benefits of WhatsApp Business use in appropriate user cases:

- Engaging with, reach out to and signpost members of the public as appropriate;
- Being part of community solutions driven by the public;
- Enabling NYP to gather intelligence and receive reports which we may not otherwise know about;
- Building working relationships with communities, thereby building confidence in the NYP;
- Saving policing resources by educating and focusing the members of the public's attention on incidents which are reportable, and those that may not be.

A case study detailing more specific benefits of WhatsApp Business use is available at **Appendix D**.

The decision whether to approve the use of WhatsApp Business within a team ought to be made by the Information Asset Owner. The decision maker should keep in mind the purpose of the platform use, the level of information which could pass through the platform and ensure that they can align appropriate resource to govern the use of WhatsApp Business.

Below are some of the key aspects that should be given consideration, and which should form part of the risk-based decision making.

- Where the data will be transferred and stored by WhatsApp Business, as this may have security and data protection implications;
- The retention and disclosure obligations of any content communicated via WhatsApp Business;

- Account set up and authentication to ensure individuals who are being communicated with are who they say they are;
- The purpose of the channels set up, the topics of conversations, and how these will interact with Facebook's membership to the National Centre for Missing and Exploited Children (NCMEC) which is a global initiative focused on content reviewing and algorithms searching for Child Sexual Exploitation content against known image signatures and/or hashing (strings of characters transformed into a shorter fixed-length value that represents the original content);
- Encryption and its known shortcomings in terms of the same version of the applications needing to be used by all users for the content to be truly encrypted;
- Auto-downloads and device syncing by users, especially members of the public, and the potential of the information to be shared with other devices and further transferred;
- Device security, especially of members of the public, in terms of security practices such as installing updates, notification configuration and visibility of messages, and whether devices are PIN locked;
- WhatsApp Business security in terms of known vulnerabilities and previous security breaches experienced by the supplier, for instance the May 2019 vulnerability being exploited which allowed spyware to be installed on users' devices;
- Future developments of WhatsApp and the Supplier, Facebook, which are seeking to create a cross-platform integration which would messages from Facebook to be sent to WhatsApp, and vice versa, but also the general fast-paced technology advancement which means new features may be rolled out and used before we can fully understand their security implications; and
- Supplier's compliance with legal obligations as Facebook have published a disclaimer to advise they provide no warranties in using the platform.

A decision-making tree aimed at IAOs is available at **Appendix E**.

Should approval for WhatsApp Business be granted, IAOs should consider using the audit scope document is available at **Appendix B** as part of the auditing requirement of the use of WhatsApp Business. An example of suitable privacy notices for WhatsApp Business chats is available at **Appendix C**; where IAOs wish to formulate their own privacy notices, the Data Protection Team must be consulted. All proposed users ought to sign the terms of use (**Appendix A**) and comply with these at all times. WhatsApp Business Set up instructions are available at **Appendix H**.

Information Asset Owners should remind the users of WhatsApp Business that the Social Media and Community Messaging Procedure applies to all WhatsApp Business engagements. Users should also be reminded that any potential or actual security breaches must be reported in line with the Security Incident Reporting Procedure to the Data Protection Officer, Information Security Officer or where necessary, Professional Standards, for investigation. Security Incidents should be reported immediately via the SecurityBreachReporting@northyorkshire.pnn.police.uk inbox or via the e-form accessible from The Source (The Source > e-forms > Information Management > Security Reports > New). Please note, using WhatsApp outside the scope of an approved business case will constitute a security incident and may carry disciplinary consequences depending on the severity of the incident.

It is important that responsible security practices are upheld in the usage of the WhatsApp platform to limit any risk to NYP and its assets. For this reason, the Force Information Security Policy and associated policies and procedures should be adhered to when using WhatsApp Business. Users are asked to be responsible and in line with the force Internet and E-mail Procedure, not open any media or internet based links which could be sent from unknown or unverified group members.

Any approved cases of WhatsApp Business use should be communicated to the Information Security Officer by the authoriser using the e-form or from The Source (The Source>Electronic Forms>Information Management> WhatsApp Approval Request> New) The following information should be provided as a minimum:

- Purpose of accepted use;
- When approval was granted;
- Confirmation that a risk analysis was conducted in line with this framework and a summary of the perceived risks, mitigations, and benefits of the use; and
- How many and which NYP users and within which department/unit have been granted access.

Responsibilities:

Officers/ Staff - To note the content of this document and related policies and procedures and take personal responsibility for the security of NYP information.

First Line Supervision - To ensure their team members comply with the content of information security related policies and procedures and take personal responsibility for the security of NYP information.

Chief Officer Team - To ensure the continued security of NYP information and assist with managing and recording risk as per established processes.

Responsibilities of the Information Asset Owner - To ensure their team members note and comply with the content of information security related policies and procedures and take personal responsibility for the security of NYP information. To act as the decision maker and ensure appropriate governance and resources are in place to effectively manage any identified risks.