POLICEBOX


# PoliceBox

Privacy Policy

# Version Control

| Issue | Date | Author | Summary of change |
|---|---|---|---|
| 1.0 | April, 2017 | Coeus | Released |
| 1.2 | November, 2020 | Coeus | Update to provisions |
| | | | |

# Distribution

This **Privacy Policy** has been authorised by Coeus Software Ltd, for distribution with the PoliceBox platform. Users, which means Authorised Users, employed by subscriber organisations (Police Forces) must read, understand, and accept the policy to use PoliceBox.

# Welcome

**This Privacy Policy has been provided to help you understand what happens to your data when you use PoliceBox or interact with us.**

PoliceBox delivers digital transformation and business change for Police Forces, quickly and simply, with the agile, no-code App Designer, making it unique to the market.

New processes can be deployed to frontline officers in days and weeks rather than months and years, without the need for mobile software updates.

Audit trails and data integrity protections come out of the box. Flexible integration capabilities connect with existing back office systems. PoliceBox is also ready to support modern integration platforms to reduce lock-in and eliminate data silos.

# Introduction

## Who we are?

We are Coeus Software Ltd (Coeus, We, Our), the developers, publishers, and promoters of PoliceBox®.

We are registered in England and Wales at: **Suite 411, Boho-5, Bridge Street East, Middlesbrough, TS2 1NY**. With company number **05830505**.

## What this agreement does?

Coeus hereby grants license to you to use:

- PoliceBox mobile application software, the data supplied with the software, (**App**) and any updates or supplements to it.
- The related online and paper documentation (**Documentation**).
- The service you connect to via the App and the content we provide to you through it (**Service**).

as permitted in these terms and the contract under which the overall Service is provided (**Master Agreement**). The terms of the Master Agreement prevail over any terms found above or below, subject to that usage being authorised by the nominated system administrator of a subscribing Customer organisation (Police Force).

**PLEASE READ THESE LICENCE TERMS CAREFULLY**

BY DOWNLOADING AND USING THE APP YOU AGREE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS DO NOT DOWNLOAD OR USE THE APP.

# App Store

## App Store Terms

The ways in which you can use the App, Documentation, and Service, may also be controlled by the rules and policies of the app store from which the App was downloaded. In the event of a conflict between these terms and the rules and policies of the relevant app store, the app store's rules and policies will prevail, subject at all times to the terms of the Master Agreement.

## How you may use the PoliceBox App

In return for your agreeing to comply with these terms you may:

- download or stream a copy of the App onto mobile devices and view, use and display the App and the Service on such devices.
- use any Documentation to support your permitted use of the App and the Service; and
- receive software code or updates of the App incorporating "patches" and corrections of errors as we may provide.

## Minimum Age Restriction

You **must** be aged **18 years or over** to accept these terms and use the App.

## Updates and Changes to the Service

From time to time we may automatically update the App and change the Service to improve performance, enhance functionality, reflect changes to the operating system or address security issues. Alternatively, we may ask you to update the App for these reasons.

If you choose not to install such updates or if you opt out of automatic updates you may not be able to continue using the App and the Services.

# License

## Device Ownership

You agree to only download or stream the App on devices as authorised and designated by your organisation - typically your organisation will be a Police Force that holds a valid PoliceBox subscription.

If you download or stream the App onto any phone or other device not owned by you, you must have the owner's permission to do so. You will be responsible for complying with these terms, whether or not you own the phone or other device.

## License Restrictions

You agree that you will:

- not rent, lease, sub-license, loan, provide, or otherwise make available, the App or the Services in any form, in whole or in part to any person without prior written consent from us;
- not copy the App, Documentation or Services;
- not translate, merge, adapt, vary, alter or modify, the whole or any part of the App, Documentation or Services nor permit the App or the Services or any part of them to be combined with, or become incorporated in, any other programs, except as necessary to use the App and the Services on devices as permitted in these terms;
- not disassemble, de-compile, reverse engineer or create derivative works based on the whole or any part of the App or the Services nor attempt to do any such things, except to the extent that (by virtue of sections 50B and 296A of the Copyright, Designs and Patents Act 1988) such actions cannot be prohibited because they are necessary to decompile the App to obtain the information necessary to create an independent program that can be operated with the App or with another program (**Permitted Objective**), and provided that the information obtained by you during such activities:
    - is not disclosed or communicated without the Licensor's prior written consent to any third party to whom it is not necessary to disclose or communicate it to achieve the Permitted Objective; and
    - is not used to create any software that is substantially similar in its expression to the App;
    - is kept secure; and
    - is used only for the Permitted Objective;
- comply with all applicable technology control or export laws and regulations that apply to the technology used or supported by the App or any Service.

## Acceptable Use Restrictions

You must:

- not use the App or any Service in any unlawful manner, for any unlawful purpose, or in any manner inconsistent with these terms, or act fraudulently or maliciously, for example, by hacking into or

inserting malicious code, such as viruses, or harmful data, into the App, any Service or any operating system;

- not infringe our intellectual property rights or those of any third party in relation to your use of the App or any Service, including by the submission of any material (to the extent that such use is not licensed by these terms);
- save for in the course of the normal use of the App, not transmit any material that is defamatory, offensive or otherwise objectionable in relation to your use of the App or any Service;
- not use the App or any Service in a way that could damage, disable, overburden, impair or compromise our systems or security or interfere with other users; and
- not collect or harvest any information or data from any Service or our systems or attempt to decipher any transmissions to or from the servers running any Service.

## Intellectual Property Rights

All intellectual property rights in the App, the Documentation and the Services throughout the world belong to us and the rights in the App and the Services are licensed (not sold) to you. You have no intellectual property rights in, or to, the App, the Documentation, or the Services, other than the right to use them in accordance with these terms.

## Termination

**IMPORTANT: WE MAY END YOUR RIGHTS TO USE THE APP AND THE SERVICES IF YOU BREAK THESE TERMS**

We may end your rights to use the App and Services at any time by contacting you if you have broken these terms in a serious way. If what you have done can be put right we will give you a reasonable opportunity to do so.

If we end your rights to use the App and Services:

- You must stop all activities authorised by these terms, including your use of the App and any Services.
- You must delete or remove the App from all devices in your possession and immediately destroy all copies of the App which you have and confirm to us that you have done this.
- We may remotely access your devices and remove the App from them and cease providing you with access to the Services.

# Privacy

## Information Collected from You

We will collect and process the following data via the App:

- **Information the App user gives to us (Submitted information)**: This is information (data) the user gives to us via the App. It includes information provided when the user shares data via the App's functions which is likely to include a mixture of personal data (names, addresses, dates of birth) and sensitive personal data (criminal records and offences relating to a person).

- the organisation using the App, and distributing it to its authorised Users, has control over the design and use of business processes within PoliceBox, to provide a field force enablement platform. Therefore, the organisation will have constructed relevant assurance documentation, including Privacy Impact Assessment.

- **Information we collect about the user's device.** When the user makes use of the App we will automatically collect the following information:

- technical information, including the type of mobile device you used, unique device identifier (for example, your device's IMEI number, the MAC address of the device's wireless network interface, or the mobile phone number used by the device), mobile network information, the device's operating system, the type of mobile browser used and time zone setting (Device Information);

- details of the use of the App including, but not limited to traffic data, and other communication data, whether this is required for our own billing purposes or otherwise (Log Information).

- **Location information.** The App may also use GPS and/or GLONASS technology to determine the user's current location. Some of the location-enabled Services require personal data for the feature to work.

## Cookies

We use cookies to help distinguish individual users of the App. This helps us to provide the user with a good experience when using the App and also allows us to improve the App. The App is not a web browser, but is a native application on the device, which creates and manages Cookies in its proprietary format. Cookies that are created are protected by encryption. When a cookie is generated by the App, it is created so that it is only useful to the User and the Device.

We use the following cookies:

- **Strictly necessary cookies.** These are cookies that are required for the operation of the App. They include, for example, cookies that enable the user to log into the app and retain key personal settings and preferences.

- **Functionality cookies.** These are used to recognise the individual user when they return to the App. This enables us to personalise the App and remember certain non-key preferences.

You can find more information about the individual cookies we use and the purposes for which we use them in the table below:

| Cookie | Name | Purpose |
|---|---|---|
| **Authentication Token** | User Profile | Used to maintain your secure access to the service. The authentication token is refreshed at routine intervals. This is safer than using your credentials. The authentication token is held in the user profile. |
| **User Profile** | User Profile | Used to maintain a local copy of your user profile for the service. Is part of the mechanism by which an 'offline' login can take place when LTE or WiFi is unavailable. |

## How we use the Information

We use information in the following ways:

- Submitted Information: to provide the Services as outlined in the Master Agreement and these terms.
- Device information: to monitor use of the App and the Services and to improve performance of the App and the Services.
- Log information: to monitor use of the App and the Services and to improve performance of the App and the Services.
- Location information: to provide the Services as outlined in the Master Agreement and these terms.

We may associate any category of information with any other category of information and will treat the combined information as personal data in accordance with this policy for as long as it is combined.

We will never disclose information about identifiable individuals to third parties, but We may aggregate and anonymise (the **anonymised data**) such information for use as we see fit.

We may associate any category of information with any other category of information and will treat the combined information as personal data in accordance with this policy for as long as it is combined.

## Disclosure

We will never disclose information about identifiable individuals to third parties unless We are under a legal or regulatory duty to disclose it.

We encrypt the data we receive from you, as you collect it. We cannot view that data while it is held in the App or Service, we will be unable to disclose it if we are any legal or regulatory duty to provide it[1].

## Where we store the Data

We use in-country Data Centres of the Microsoft Azure Cloud platform to host the Service. For Police Forces in the United Kingdom, this means that the data that We collect via the App will not be transferred to, or stored at, a destination outside the United Kingdom of Great Britain and Northern Ireland.

[1] Data Retention: It is important that Customers ensure that they have proper data retention periods in place, to encompass the data which is passed to the Customer from the Service. The Service removes the data from itself when it has been delivered to the Customer.

Unfortunately, the transmission of information via the internet is not completely secure. Although We employ industry standard techniques to protect the data transferred via the App, using a layered approach, any transmission is at the user's own risk. Once We have received the information, We will use strict procedures and security features to try to prevent unauthorised access. Except for the anonymised data, We are unable to view any of the information you collect using the App or Service because of the data protection mechanisms we have put in place.

# Business Operations

## Changes to these or any Terms

Any changes We may make to our terms in the future will be notified to your organisation, by e-mail or when you next start the App. The new terms may be displayed on-screen or you may be redirected to a website, and you may be required to read and accept them to continue your use of the App or the Services.

## Sub Processors

In addition to the above relating to your use of the App, We use certain sub-processors for the general running of our business, such as for sales & marketing, support, or billing. We take all reasonable steps to ensure We satisfy the UK Government's Data Protection Act (DPA 2018) incorporating the provisions of the E.U. General Data Protection Regulation (GDPR 2018), such as:

- Process data in accordance with our Information Security Policy and system specific instructions;
- Ensure that only persons authorised to process the data are able to do so, and that they have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Not engage a sub-processor without prior specific or general written authorisation of Coeus Software Ltd, where the relevant checks have been undertaken and risk assessment put in place, including the imposing of same data protection obligations as are in place between Coeus and our Customers;
- Provide regular training in security and data protection to personnel to whom are authorised and permitted access to personal data;
- Implement and maintain appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data, in accordance with our Information Security Policy;
- Have measures in place that permits and encourages reporting of potential breaches, including a whistle-blowing policy;
- Cooperate in deal with legal and regulatory requests from Our clients, data subjects or data protection authorities, as applicable.

Where the sub-processor is a Cloud-based IT system, We adopt the relevant Data Processing Addendum, including the ensuring of compliance with technical measures, including the use of multi-factor authentication and role-based access to capabilities.

Where the sub-processor is a direct supplier (such as a developer-partner), that supplier must adhere to the above requirements in relation to organisational and technical security measures to safeguard Information Assets.

Our list of sub-processors (as well as other similar content about the PoliceBox platform) may be found online, in the Sub-Processors statement, via the PoliceBox Knowledgebase (https://kb.policebox.com/policebox)

COEUS
software

Suite 411, Boho-5
Bridge Street East
Middlesbrough.  TS2 1NY

servicedesk@coeussoftware.com