

WATSMobile

System Overview

And

Options for Implementation

1. Purpose of this document

This document describes in general terms the functionality of WATSMobile and options for the implementation of the system for Court Areas.

2. Overview of System

WATSMobile is a web-based system which permits authorised access to information relating to Warrants issued by Magistrates' Courts.

Access is via a standard web browser, such as Internet Explorer, with restrictions on facilities by use of a log in name and password.

Warrants are issued by business processes effected by Magistrates' Courts and mainly comprise of two types

- Financial Warrants e.g. for non payment of fines
- Bench Warrants, e.g. for non appearance at court following a charge or summons

Details of Warrants issued by the business processes of the Courts are available to WATSMobile in an electronic format which a user can then import into the WATSMobile database. This document does not cover the business processes or generation of files by the two main Magistrates' Courts Computer Systems, Libra and Fujitsu's MCS.

During the import process details of a defendant's surname, forename and date of birth are matched against existing records to collate all warrants for that person wherever they may have been issued.

This core defendant and warrant data can then be updated by the addition of warning signals, notes or payments. Warrants can be issued to individuals, such as a Bailiff Company or to enforcement officers by automatic address matching against allocation areas.

Warrants for breach of a probation or community service order can be manually added to the system, linking to defendants with financial or non appearance warrants if appropriate.

The updating of warrant cancellations or payments is a manual process by users using data from the Libra application as there is currently no cancellations file available. Fujitsu MCS cancellations are automatic on import of a file.

Details of cancelled warrants are held by WATSMobile together with any notes, warning signals or allocations to provide a complete history should further warrants be issued against the defendant.

Advanced searching assists in providing statistics and bulk allocation or cancellations of warrants by a number of parameters.

3. Protection of Data.

Secure Sockets Layer (SSL) cryptographic protocols provide secure communications for data transfer between the user's workstation and servers.

Access to facilities within WATSMobile is controlled by the use of a login and password.

Varying roles are created within the system provide for:-

- the ability to update defendant or warrant information
- read only permission to defendant or warrant data
- allocation of warrants to enforcement officers
- recording of payments against warrants
- cancellation of warrants
- the addition of notes or warning signals
- uploading of Libra or Fujitsu MCS files
- user and role management

A user can also be immediately manually excluded from the system should their login details be compromised.

Users can amend their own passwords with the next major revision of the software (Revision Number 3.0) to include a demand that a password contains both upper and lower case characters and at least one digit. Passwords will need to be amended after defined period, this being a system parameter.

WATSMobile also times a user out of the system after a 30-minute period of inactivity.

An additional security feature of the system is the use of I.P Address checking. WATSMobile can detect the I.P address of an incoming log in and check against a table of valid I.P addresses. This validation table can contain single I.P addresses or a range of I.P addresses.

Should an attempt to be made to access the system from an unauthorised I.P address, the user is denied access and an automated email is generated to Specialist Computing Support who then follow the action by a call to the main nominated user contact.

It should be noted that this I.P address checking can only be effectively invoked where Static I.P addresses are generated, which is the case on the Libra Office Automation Network.

4. Role Management

WATSMobile utilises a concept of users and role management. A user is allocated a series of roles, e.g. Admin, local admin, defendant admin, diary admin. Additional data roles are created for each Court Area which has data deployed in the database. Thus, for a example, a user who has been allocated a data role of "Wiltshire" would be able to see all the defendant and warrant information for Wiltshire. Should, for example, Dorset Court Area Data be held in the same SQLServer database a Wiltshire user who has been given the additional role of "Dorset" would also be able to interrogate data for the Dorset Court Area.

Current Roles within WATSMobile – excluding the Court Area data roles are:

- Admins – control of users and configuration of the whole database
- LocalAdmins – control of users and configuration for their own nominated court area
- Users – standard read only access to data within the database
- Allocations – Users who can be allocated and view warrants
- Allocationadmins – can control the allocation of warrants to users
- DataTransfer – can import warrant data
- Defendant Admins – can amend defendant and warrant data
- DiaryUsers – Can update their own Enforcement Officer Diary
- DiaryAdmins – can administer and view diary entries for all diaryusers
- ExportData – can export data into a spreadsheet based on their chosen search criteria
- Officers are listed in the allocations table and may add notes to a defendant but not amend the defendant or warrant details
- Restricted – All captions describe entries as "Fines" and not "Warrants". This role is intended for Police users who are not required to deal with the arrest or detention of a defendant but only be aware that the defendant has previously defaulted on fine payments for the purposes of Conditional Cautioning.

5. Key Data held by the system on Defendants and Warrants.

- Defendant
 - Surname
 - Forename(s)
 - Sex
 - Date of Birth
 - Address
 - Post Code
 - Warning Signals
 - Free Text Notes
- Warrant
 - Warrant Type
 - Warrant Number
 - Date of Issue
 - Value
 - Allocated to
 - How Completed
 - Date Completed
 - Completion Notes

6. Deployment of the System

The key features relating to the deployment of WATSMobile are:

- No software is required to be deployed on user Workstations other than a standard browser. E.g. Internet Explorer Versions 6 or 7. Specialist Computing would not expect to deploy the browser
- WATSMobile has successfully been accessed through the Libra Office Automation network, including the use of I.P Address Checking and restrictions
- No Cookies are deployed on the users Workstations
- Standard Internet Explorer Features such as adding the site to Favourites or browser history continue to work effectively.
- Upgrades to the software can be deployed centrally by Specialist Computing following notification to the Court Areas.
- The maintenance of new users for a court area can either be undertaken by an administrator in the Court Area or by Specialist Computing on their behalf
- Telephone Support for the application and system usage is maintained with Specialist Computing
- User Access to the system can be given to other agencies such as the Police Service with the approval of the Court Service. Again, no software needs to be deployed on the Police infrastructure.