

WATCH PERSONAL DATA HANDLING STATEMENT

1. Thames Valley Police Force holds the personal data of certain members of a variety of Watch schemes, such as scheme co-ordinators, on a computer database. This personal data consists of:
 - Name, address, telephone and/or fax numbers, email address
2. The personal data held by the police will be used for:
 - Preventing and detecting crime.
 - Giving assistance to Watch Schemes and other Community Groups in accordance with Force policies and procedures.
3. The data will be used by:
 - Police personnel for the purposes described at 2 above, within the terms of the Thames Valley Police Force's notification with the Office of the Information Commissioner.
 - In the case of Neighbourhood Watch, the Thames Valley Police Neighbourhood Watch Association is legitimately permitted to hold personal data for the purposes of providing support to Neighbourhood Watch.
 - Thames Valley Police use an outside company for the supply and maintenance of the Ringmaster system. All data is stored on their computer systems on behalf of Thames Valley Police. All possible security measures are taken to protect your information at all times.
4. The data may be passed to:
 - The National Neighbourhood Watch Association, Neighbourhood Watch Support Groups, Watch Associations or Thames Valley Police Volunteers not holding separate Data Protection Notifications, whilst working in partnership with the Police, for the purposes described at 2 above.
 - Co-ordinators from schemes adjacent to yours held within the geographic area supported by your Thames Valley Police Watch Administrator. The Thames Valley Police Force will not, however, divulge any personal data to prospective members within a scheme area or where the co-ordinator is operating a covert scheme. Under these circumstances, persons seeking to contact a Neighbourhood Watch Scheme will have their name, address and telephone number taken and then passed on to the relevant co-ordinator for them to make contact with the enquirer direct.
5. Once placed on to the database, the personal data can only be accessed by authorised users of the system. Computers are password protected.
6. The database is updated as and when inaccuracies are identified in the course of ongoing liaison, and in any case will be subject to a full audit at least every four years.
7. Nothing contained in the Statement affects any local agreements where scheme co-ordinators or others have entered into agreements, which make their personal data more widely available.
8. Personal details will not be disclosed to any commercial organisation.

Protection of Personal Data

The unauthorised use or disclosure of personal data is a criminal offence under the Data Protection Act 1998 and the Computer Misuse Act 1990.