

ACPO
Crime and Disorder Reduction and Partnership
Sub-Committee



POLICING AND WATCH SCHEMES
GUIDANCE ON INFORMATION SHARING

August 2001

Foreword

Issues of information sharing and data protection relating to Watch Schemes are frequently raised by police and Neighbourhood Watch. These issues are seen as complex and have hindered the sharing of information between the police and watch schemes.

A survey of the way Police Forces share information with watch schemes (Summer 2000), indicated a wide variety of practices across the country. The main finding of the survey was that information was widely shared, but different Police Forces experienced different problems in doing this. The conclusion drawn is that difficulties in sharing information are often not universal and linked to legal issues, but are localised and linked to working practices.

This guidance aims to address those localised issues, drawing on good practice from across the country, to provide a reference point for staff seeking to share information and for Force Data Protection Officers. It has been developed over time in close co-operation with The Office of the Information Commissioner, the Home Office, the National Neighbourhood Watch Association, the ACPO Portfolio Group on Data Protection and several individuals who have had a very useful input.

Whilst it is hoped that the guidance will answer the most frequently asked questions, it is inevitable that such guidance will continue to evolve over time. Indeed, the original document produced by Derbyshire Constabulary has now been amended to take into account the provisions of the Data Protection Act 1998, which came into force on 1 March 2000, and the Human Rights Act 1998.

F N Whiteley
Assistant Chief Constable
Northamptonshire Police
(on behalf of ACPO Crime and Disorder Reduction and Partnership Sub-Committee)

August 2001

Contents

	<i>Pages</i>
POLICING AND WATCH SCHEMES GUIDANCE ON INFORMATION SHARING	2-7
Appendices	
A. Flowchart for disclosing information	8
B. Model Code of Practice for volunteers at Police premises	9
C. Vetting Watch Co-ordinators - ACPO policy	10
D. Guidance notes for police considering the services of volunteers at police premises	11-13
E. Model Watch Scheme Registration Form and Data Handling Statement.	14-15

POLICING AND WATCH SCHEMES: GUIDANCE ON INFORMATION SHARING

1. Purpose

- 1.1. The purpose of this guidance to provide clear outline advice and good practice for the Police Service regarding information sharing with Watch Schemes. It deals with issues surrounding the disclosure of information to Watch Schemes and the disclosure of Watch Schemes details to third parties.

2. The relationship between the Police and Watch Scheme

- 2.1. There are now many types of Watch Schemes in existence. They are often made up of members of the public or business community and are primarily established to prevent and detect crime and disorder in a local area. Watch Schemes in most circumstances cannot be regarded as an agency of the police or as an organisation accountable to the police. Many are represented by scheme co-ordinators, although in some instances schemes are organised into local associations.
- 2.2. Watch schemes can be vital partners of the police in the fight against crime. Their role in preventing crime, supporting victims and detecting crime is a key one. To ensure their effectiveness, details of crimes and incidents may be passed to co-ordinators and scheme members. In the vast majority of cases this information will be depersonalised information on crime patterns and trends, as well as general crime prevention advice.
- 2.3. **Since the law does not regulate the disclosure of such depersonalised or anonymised information there should be few issues to consider before disclosing.**
- 2.4. Particular care should be taken in cases where Watch members work with the police as Support Groups (often from police premises), to disseminate crime information to scheme co-ordinators/members. It is circumstances such as these, where the handling of personal data may become an issue.

3. Disclosure of Information

- 3.1. The police have an important and general power at common law that allows them to disclose information as and when appropriate. As an established and accountable organisation they hold and disclose personal data for the primary purposes of:
 - (a) the prevention or detection of crime; and/or
 - (b) the apprehension or prosecution of offenders.

3.3. The fair and lawful handling of personal information is dealt with in both the Data Protection Act 1998 and the Human Rights Act 1998. It is essential, if the Police Service is to retain the confidence of the public in their use of the information it holds that the principles of these Acts are observed.

3.4. The Data Protection Act 1998

The Data Protection Act 1998 exists to ensure that personal information is processed and handled in a fair and lawful way. Anyone dealing with personal information must comply with the eight enforceable principles of good practice. They say that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to other countries without adequate protection.

The Act also contains certain exemptions, some of which relate to the prevention or detection of crime, or the apprehension or prosecution of offenders. These exemptions will permit the disclosure of personal details in particular cases without an individual's consent. However, these are not blanket exemptions from the need to obtain such consent and are only available on a case by case basis where there would be a real likelihood of prejudice to crime prevention and detection matters if disclosure did not occur.

3.5. The Human Rights Act 1998

The general purpose of the Human Rights Act 1998 is to protect human rights and fundamental freedoms and to maintain and promote the ideals and values of a democratic society. Article 8, "The Right to Respect for Private and Family Life, Home and Correspondence", is relevant when it comes to the disclosure of personal information. The Act makes it clear that public authorities may only interfere with someone's private life where they have legal authority to do so, the interference is necessary in a democratic society for one of the aims stated in the Article and is proportionate to that aim. (The prevention and detection of crime is one of those aims).

3.6. A flowchart has been designed to assist in dealing with the disclosure of information – see Appendix A.

4. Disclosure of information to Watch Schemes

- 4.1. As previously stated, the disclosure of general depersonalised crime and incident information is not covered by the Data Protection Act. Therefore, messages that state, for example, '*during the night in the past week there has been a series of shed burglaries on Spencer Avenue etc'* are not an area of contention.
- 4.2. There may of course still be issues to consider before releasing such information (see 4.10). A useful guiding principle here is, if the information has been or could be released to the public via the press then there should be no issues with the release of such information to Watch schemes.
- 4.3. Regarding the disclosure of personal information, in the context of this guidance, this could be in relation to a victim of crime, a suspect, an offender or a member of a Watch scheme.
- 4.4. In relation to victims of crime an obligation of confidence exists between the police and the individual and this places a restriction on disclosing personal information for purposes other than which it was provided. A victim should be informed as to what the data is to be used for, including to whom it might be disclosed.
- 4.5. In the rare circumstances where it may be necessary to disclose personal information to Watch schemes about victims, such information needs to be treated with the utmost sensitivity and disclosure of some types of crime victimisations to Watch Schemes would be inappropriate. Therefore, a number of criteria should guide disclosure policies.
- 4.6. The first point to be considered relates to the victim's consent and the essential question is, "*Has the victim consented to the disclosure?*". Disclosures of personal information can be made if explicit consent from an individual is given. Without consent, the disclosure of personal information to Watch schemes in respect of crime or incidents would need to be justified for either specific crime prevention or detection purposes.
- 4.7. The justification for the disclosure *without consent* must be that there would be a substantial chance, rather than a mere risk, that in the particular case the prevention or detection of crime, or the apprehension or prosecution of offenders would be prejudiced. The important question to ask is, "*Will the failure to disclose personal data in this case be likely to prejudice the prevention or detection of a crime or the apprehension or prosecution of offenders?*"
- 4.8. The third criterion relates to confidentiality and sensitivity, and its application requires professional judgement. The key question here is, "*Will disclosure of this information cause distress or embarrassment to the victim?*"

- 4.9. There is no one rule to apply when considering the disclosure of information to Watch schemes or indeed to the general public. Each disclosure must be treated individually and assessed on a case by case basis. Several things should be taken into consideration:
- Is there a legal basis for disclosure?
 - Is the information sensitive?
 - Will the failure to disclose personal data in this case be likely to prejudice the prevention or detection of a crime or the apprehension or prosecution of offenders?
 - Is the disclosure likely to cause any distress? (Particularly if the information is about a victim of crime).
 - Will it raise the fear of crime?
 - Proportionality? What is the least intrusive option?
- 4.10. All such disclosure should be fully evidenced. Policies and procedures that reflect these criteria will meet the requirements of the both the Data Protection and Human Rights Act.
- 4.11. There should be similar considerations made with regard to suspect or offender details. However, it is likely in most cases that consent would not be sought, on the grounds that it would prejudice the investigation. So for example, passing details of suspect vehicles, including registered numbers, for the purposes of preventing and detecting crime, does not contravene the provisions of the relevant Acts.

5. Watch Scheme members as volunteers assisting the Police

- 5.1. In some cases co-ordinators and scheme members work as part of a 'Watch Support Group' in police premises. Their role includes communicating crime information to other Watch Schemes in an area. Usually, this is likely to be general, depersonalised information. However, as they are working within police premises they may come into contact (directly or indirectly) with personal data. As a result and to overcome any restrictions which would diminish their effectiveness or create conflict regarding the use of sensitive information their role and responsibilities need to be clearly defined. (See Appendix B: Model Code of Practice for volunteers at Police premises).
- 5.2. Where members of Watch Schemes are to undertake specific tasks involving data protection issues, clear policy guidelines and training should be provided for the volunteers and monitoring systems should be in place. The ACPO policy on vetting Watch Co-ordinators states that, where Watch Co-ordinators or volunteers have access to police premises, as part of a support team or similar, it is a sensible security measure to 'vet' such people. (See Appendix C: ACPO Policy on Vetting Watch Co-ordinators).

- 5.3. Under the Data Protection Act 1998, volunteers may be criminally liable if they obtain or disclose personal data held by the Chief Constable without his or her authority. (See Appendix D: Guidance notes for Police Considering the Services of Volunteers at Police Stations).
- 5.4. It is therefore recommended that all members with such access should be subject to vetting (such as a “Counter Terrorist Check” or other local checks in accordance with Force policy).
- 5.5. A blanket approach to vetting other Watch co-ordinators may be an onerous and costly task and may not be based upon real need. Vetting of co-ordinators is a matter for individual Chief Constables to decide in accordance with local concerns and need. However, it is acknowledged that Watch co-ordinators need to be trusted and respected by the community they serve. It is also important that they have the confidence of police, other partner agencies and that they do not pose a risk to the community by being in put in a position of trust. These all support the argument to carry out vetting as a safeguard. The associated costs should be weighed against the potential risks.

6. Disclosure of Watch details

- 6.1. A further area for consideration is the disclosure of personal information of Watch Scheme members. Generally, this should be treated in the same way as all other personal information the Police Service holds. However, due to the community nature of many Watch Schemes it is often necessary for details of Watch co-ordinators for example, to be passed on to others to be contacted about the scheme or for a specific operation or initiative.
- 6.2. It is recommended that authorisation is sought when personal details of new Watch Scheme members are taken to be retained by the Police and a statement which specifies those to whom the data will and may be passed to. In most circumstances this would be as a point of contact for local purposes, such as to Watch Support Group initiatives. It would also be advisable to include any National Associations who may wish to make contact with scheme members. (See Appendix E: Model Watch Scheme Registration Form and Data Handling Statement).
- 6.3. When disclosing Watch details to a third party, it is vital that the purpose for doing so is clearly established. It may be necessary for an agreement or protocol to be signed between the police and those receiving the information. This should state that the disclosure of the information has been given with the consent of the Watch member and will be handled in a fair and lawful manner, in accordance with the individual’s rights, not kept for longer than necessary and kept secure.

- 6.4. If unsure, contact the Watch member first before disclosing their information. Unless explicit consent has been obtained from the Watch member, such an agreement should also state that the information should not be passed on to any other party.

7. Information disclosure through other Watch structures

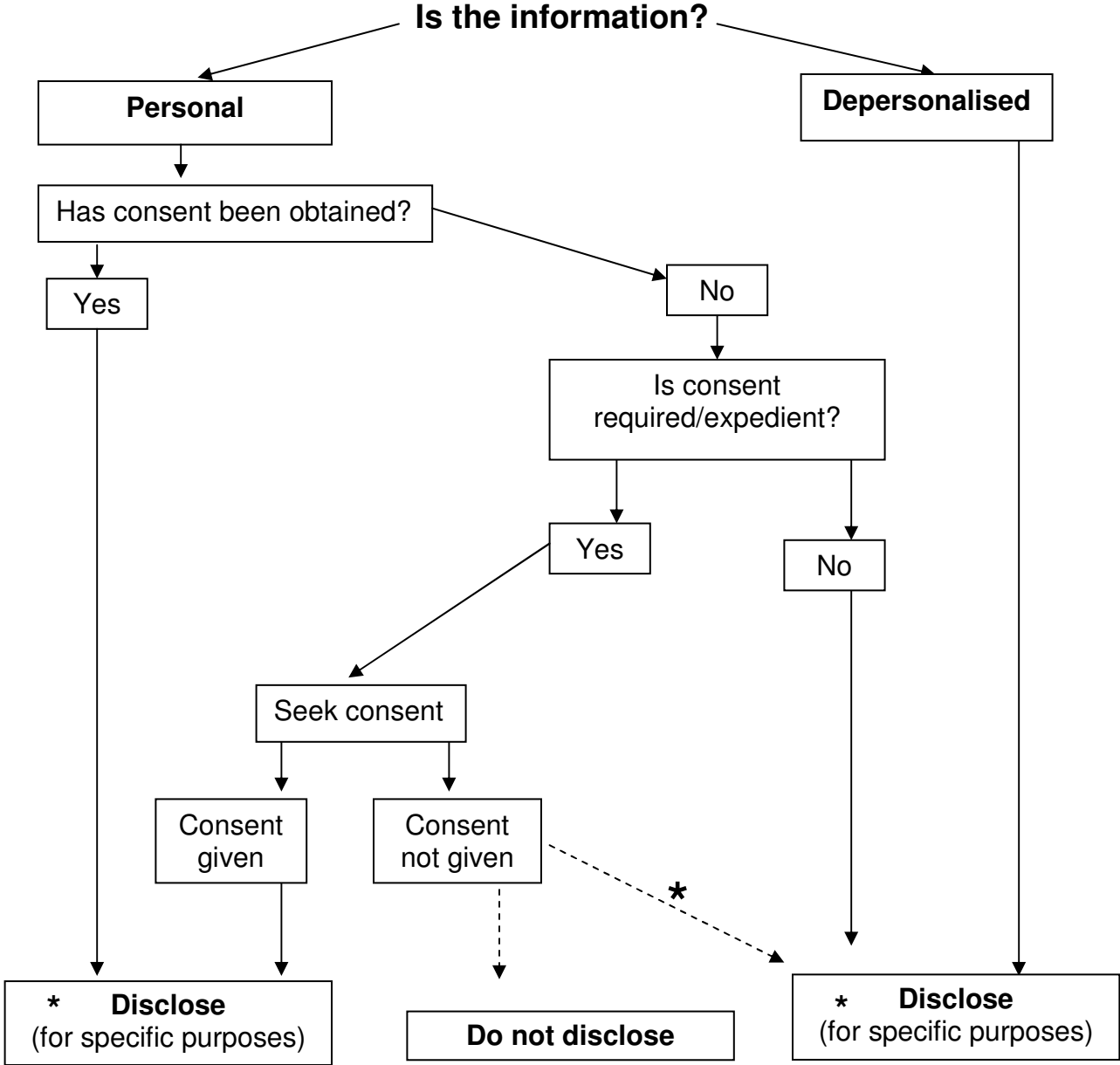
- 7.1. In some areas, other organisations may be responsible for the distribution of information to assist in the prevention and detection of crime. Local authorities, for example, have established Neighbourhood Watch units with dedicated staff responsible for communicating with Watch Schemes. These take away much of the administrative work carried out by existing police departments or staff specifically employed by the police for this purpose.
- 7.2. Wandsworth Council in London is a good example of this type of arrangement. They adhere to all of the data protection guidelines mentioned and have a strict code of practice for dealing with the passing of information. (see Watchlink crime bulletin at www.wandsworth.gov.uk/watchlink)
- 7.3. When it comes to the disclosure of information to a Local Authority, or any other relevant organisation, this should be dealt with in the same way as information given to a Watch Scheme or co-ordinator. These special relationships should not assume any exemptions from data protection legislation. Information should be “depersonalised” before being shared and a clear code of practice or protocol drawn up to govern the type of information and manner in which it is to be used. It would be useful to circulate this guidance to such organisations for their information.

8. Further Guidance

- 8.1. Most Police Forces have produced, in co-operation with Watch Schemes in their area, procedural, policy or good practice guidance for dealing with the workings between the two organisations. It is recommended that these should contain some of the advice given in this guidance.
- 8.2. Information about the Data Protection Act 1998 can be found on the website of the Office of the Information Commissioner: **www.dataprotection.gov.uk**. In addition, a useful piece of guidance has been produced by the Information Commissioner for members of Watch Schemes. This can be obtained by contacting the Commissioner’s office.
- 8.3. Further advice can be obtained from your Force Data Protection Officer.

FLOWCHART FOR DISCLOSING INFORMATION

- Before disclosing any personal information (whether consent has been given or not) the following points should be taken into considerations: *
- Is the purpose for disclosure/non-disclosure clear?
 - Will the failure to disclose personal data in this case be likely to prejudice the prevention or detection of a crime or the apprehension or prosecution of offenders?"
 - Has it got a legal basis?
 - Is it necessary?
 - Is it proportionate?
 - It is likely to cause distress?
 - Will disclosure or failure to disclose be likely to prejudice any police activity?



Sample Code of Practice for volunteers at Police premises

Welcome to (Force name)

The Data Protection Act 1998 places a personal legal liability on those who hold or use personal information about living individuals on information storage systems.

Like you, the Chief Constable has responsibilities one of which is to restrict access to and disclosure from such systems. That is why you, in common with all members of staff have access to our information systems on a restricted basis.

Here are some working guidelines about the disclosure of information:

- Do remember that much of what you see and hear whilst you are with us is confidential and you should not talk about what you see or hear when you are away from the police environment
- Only release personal information that you have been told you could release and only release it in accordance with the instructions you have been given.
- You must not use any information that comes to your notice whilst you are with us, for any other purpose. If you do you may commit a criminal offence for which you personally are responsible.
- It is not anticipated that a volunteer will have direct access to information systems holding personal information about individuals

If you have any queries or would like further information contact

..... who is responsible for ensuring your use of information falls within our guidelines.

Alternatively, contact the Force Data Protection Officer on

Thank you for volunteering to help the community.

Please sign the receipt at the bottom of this page to confirm that you have read and understood and accept the guidance shown above.

To: Data Protection Officer, Headquarters

I confirm that I have read, understood and accept the “Guidance to Community Volunteers on Data Protection Issues”

Name: _____ Area: _____

Signature: _____ Station: _____

Vetting Watch Co-ordinators - ACPO Policy

Where Watch Co-ordinators or volunteers have access to police premises, as part of a support team or similar, it is a sensible security measure to 'vet' such people.

In addition, where there are data protection issues the guidance developed by ACPO (See Appendix D: Guidance notes for Police Considering the Services of Volunteers at Police Stations) is relevant.

A blanket approach to 'vetting' other Watch co-ordinators would be an onerous and costly task not based upon real need. Vetting of co-ordinators is a matter for individual Chief Constables to decide in accordance with local concerns and need. However, it is acknowledged that Watch co-ordinators need to be trusted and respected by the community they serve. It is also important that they have the confidence of police and other partner agencies. It is also important that they do not pose a risk to the community by being in a position of trust.

Community and criminal intelligence should provide indicators that provide such a risk profile. Where there are adverse indicators, each case would have to be judged on an analysis of the risks. A criminal conviction on its own may not be sufficient reason for disqualifying a person from becoming a co-ordinator. Factors, including the type of offence, the seriousness of the offence, the length of time since it was committed, all have relevance to decision making.

ACPO CPSC 04.11.99

Guidance Notes for Police Considering the Services of Volunteers at Police Premises

These guidance notes have been prepared to assist Chief Officers in considering the issues relevant to the services or volunteers in police premises.

1. Introduction

1.1 The key role that the volunteer has to play in community safety partnerships is well acknowledged. However, there are a number of issues which need to be considered such as the Chief Constable's/Volunteer's legal relationship.

1.2 Under the Data Protection Act 1998, volunteers may be criminally liable if they obtain or disclose personal data held by the Chief Constable without his or her authority. This means that if a volunteer discloses, to a third party, information about an individual that they have learned about during the course of their work for the Chief Constable, they may be prosecuted for a criminal offence. Section 55 (1) of the Act, states that: -

'A person must not knowingly or recklessly, without the consent of the data controller

- a) obtain or disclose personal data, or the information contained in personal data, or*
- b) procure the disclosure to another person of the information contained in personal data'.*

1.3 Whilst this places criminal liability with 'any person', the Office of the Information Commissioner are of the opinion that Chief Officers who are not able to prove in sufficient depth the *mens rea* of individuals committing offences under the Act, will themselves be personally liable. If a Chief Constable sets up his or her relationship with volunteers as advised, it is more likely that these elements of the offence can be made out. This means that the volunteer may be prosecuted rather than the Chief Constable receiving an enforcement notice from the Commissioner for a breach of one or more of the Data Protection principles.

1.4 In view of the difficulties in fulfilling all of our legal obligations in respect of data protection, duty of confidence and sub judice issues, it is the recommendation of the ACPO Data Protection Portfolio Group that Chief Officers do not allow persons to operate police information systems unless they can be deemed his/her 'servants or agents'. This requires a legally binding contract between the Chief Constable and the volunteer.

2. Guidance and Best Practice

- 2.1. There is a wide diversity of systems used by police forces to collect information in connection with the detection and prevention of crime. Much information is available for use by other agencies in the fight against crime and to ensure the safety of the public.
- 2.2. The partnership between police and public through organisations such as 'Watch' schemes and Community Safety schemes can be exploited and made more effective. In many cases Police forces are increasingly using volunteers in a number of roles.
- 2.3. The risk of harm to individuals from a breach of security must be considered and appropriate preventative measures put in place:
 - Appropriate measures should be taken to prevent unauthorised access to or unauthorised disclosure of personal data to comply with the Data Protection Act 1998.
 - Regard shall be had to the risk of harm to individuals from a breach of security and appropriate measures put in place to prevent this.

The following paragraphs should be regarded as 'best practice'.

- 2.4. In the interest of security Chief Constables may wish to satisfy themselves that a volunteer working in police premises is a suitable person. Hence the need to carry out adequate vetting.
- 2.5. To become a servant of a Chief Constable it is necessary to establish a legally binding agreement in order to create a contractual relationship between the Chief Constable and the community volunteer.
- 2.6. Chief Constables should be aware that if a written agreement is entered into with a community volunteer then this may not be binding for two reasons:-
 - The written agreement may not be a legally binding agreement because no consideration has been given by either party. Although consideration is an essential element of a legally binding contract in English law, it is not limited to money. However, consideration must be something more than mutual benefit. The absence of payment of wages points to a lack of consideration.
 - In case of dispute, a court or tribunal will look to the facts of the relationship - the parties cannot alter the truth of their relationship by putting a different label on it.
- 2.9. There are some points which a Court or tribunal may ask in a disputed case:-
 - i. Are wages paid?
 - ii. Does the data controller (i.e. Police) have the right to suspend or dismiss the individual?
 - iii. Does the data controller have the right to exclusive service from the individual?

- iv. Does the data controller have the right to require the work to be carried out on their own premises?
- v. Does the data controller own the tools or the means of production?
- vi. Does the data controller bear the risk of loss?
- vii. Is the individual's work an integral part of the data controllers business?
- viii. Have the intentions of the parties been put into a formal written agreement or contract?

2.10 Should a Chief Constable consider that there is a legally binding agreement with a community volunteer then the following points will need to be addressed.

2.11 In most cases depersonalised information will be given by Police personnel for use by volunteers. However, should a volunteer be used to extract personal information from police information systems, typically to enable this information to be passed to 'Watch' and Community Safety Groups then:-

- i) their access to such systems must be limited to that which is necessary to enable them to carry out the task;
- ii) they must be given training in the use of such information, appropriate to their use of that system;
- iii) they must be given training in the data protection implications;
- iv) they must be given written guidelines on disclosure matters;
- v) a line-manager must be appointed with specific responsibility for such volunteer to ensure that the Police Service manages its responsibility for the security of the personal information and the training needs of the volunteer;
- vi) there should be an understanding that the personal information involved is confidential and that any breach of confidentiality will immediately lead to the termination of the individual volunteers attachment and the suspension of agreement to take further volunteers from that group.

Model Watch Scheme Registration Form and Data Handling Statement**Watch Scheme Registration Form****Personal Details**

Name: (Mr/Mrs/Miss/Ms) _____

Address: _____

_____ Postcode: _____

Telephone Number (incl. STD code): (_____) _____

Fax. Number: _____

E-mail address: _____

Scheme

Name of Scheme: _____

Position: Co-ordinator [] Deputy Co-ordinator []**Message acceptance times**

I would be prepared to accepted messages during the following times:

1. All day 8am – 9pm []
2. Between 8am – 12 noon []
3. Between 12 noon – 9pm []
4. Between 6pm – 9pm []
5. Any other period (please specify) from _____ to _____

Authorisation

I give XXXX Police the authority to place my details on a computerised database. I also agree to receive automated telephone calls that are generated by XXXX Police Messaging System. I understand that my details may be supplied to a third party but only in accordance with the Watch Personal Data Handling Statement, which I have read.

Signed: _____ Date: _____

Watch Personal Data Handling Statement

1. XXXX Force/Constabulary holds the personal data of certain members of Neighbourhood Watch, such as scheme co-ordinators, on a computer database.

This personal data consists of:

- Name, Address, Telephone and/or fax numbers, E-mail address

2. The personal data held by the police will be used for:

- Preventing and detecting crime; and
- Giving assistance to Neighbourhood Watch in accordance with Force policies and procedures.

3. The data will be passed to:

- Police personnel for the purposes described at 2 above, within terms of the XXXX Force's/Constabulary's notification with the Office of the Information Commissioner.
- The Police recognised Neighbourhood Watch Association for your area, if it is legitimately permitted to hold personal data for the purposes of providing support to Neighbourhood Watch.

4. The data may be passed to:

- The National Neighbourhood Watch Association, trained volunteers, Neighbourhood Watch Support Groups or Associations, not holding separate Data Protection Notifications, whilst working in partnership with the Police, in police premises for the purposes described at 2 above.
- Householders within the boundaries of your scheme or co-ordinators from schemes immediately adjacent to yours. The XXXX Force/Constabulary will not, however, divulge any personal data where there is doubt about the validity of the enquirer. 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 onto the database, the personal data can only be accessed by authorised users of the system. Computers are password protected and situated in police premises.

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 without the prior consent of the individual concerned.

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.