Bracknell Forest Partnership

Community Safety Partnership

Information and Data Sharing Protocol

FOREWORD

It is the legal duty of all staff in partner organisations to share information that may help prevent or detect crime or disorder. This duty is set out in the Crime and Disorder Act 1998. The effective and timely sharing of information is essential to deliver high quality services focused on the needs of the individual. In Bracknell Forest, we encourage a culture where information is shared with confidence as part of routine service delivery.

This protocol explains the terms under which partner organisations have agreed to share information and the practical steps that need to be taken to ensure compliance with those terms. Partner organisations are fully committed to share information and have agreed to comply with the procedures as set out in this protocol.

The absence of a protocol should not prevent sharing information. If you need to share information outside of the terms of this protocol or with agencies that are not party to this protocol, you should follow the guidance as outlined in Appendix A: Simple Guide to Sharing Information.

THE GUIDING RULE IS: IF YOU NEED TO SHARE INFORMATION IN ORDER TO PROTECT SOMEONE FROM HARM OR CRIMINAL ACTIVITY, YOU MUST DO SO.

Log of Revisions

Date	Version	Alterations	Author
25 July 2002	1	Not previously noted	CDRP
27 January 2003	2	Not previously noted	CDRP
21 July 2005	3	Not previously noted	CDRP
1 July 2008	4	Not previously noted	CDRP
1 April 2010	5	Clause 4: Parties to this Protocol Clause 17: Accountability Clause 18: Closure/Termination of Agreement Appendix 1: Parties to the Protocol Appendix 2: Designated Officers	Alison Koen (Community Safety Officer) in consultation with the CDRP.
8 July 2011	6	Name Change from CDRP to CSP Amendments to Appendix 1 and Appendix 2	Alison Koen (Community Safety Officer) in consultation with the CSP.
July 2012	7	Foreword 2. Definitions 3. Legal Framework 5. Responsibilities 6. Liability 7. Management and Operation of the Protocol 8. Information Sharing in Practice: What to Consider 9. Information Sharing in Practice: What to Do	Alison Koen (Community Safety Officer) in consultation with the CSP.

CONTENTS

List of Appendices

1 INTRODUCTION

The sharing of information relating to crime and disorder between organisations is vital to ensure co-ordinated and seamless provision of services that are protective and supportive. The Bracknell Forest Community Safety Partnership (CSP) recognises this and has therefore established an arrangement and procedure protocol to address this need. The benefits of information-sharing are:

- Better informed decision-making
- Improved inter-agency working
- Better profiling of crime and disorder activity and individual need or risk
- More effective intervention, support and targeting of resources
- Improved protection of individuals at risk
- Reduction in crime and disorder

2 DEFINITIONS

2.1 Information

2.1.1. Information sharing

Information sharing involves a physical exchange of information between one or more individuals or agencies. Data exchange seeks the same end but relates more specifically to information recorded in a form that can be processed automatically, usually electronically, in response to specific instructions. Any disclosure of personal information must be bound to both common and statute law, as described in this section.

2.1.2 Confidential information

Confidential information is covered by the common law duty of confidence. It applies to any information that has been received or accessed in circumstances where it is reasonable to expect that the information will be kept secret or should only be shared with a limited number of specific people.

2.1.3 Personal data

Personal data is defined under the Data Protection Act 1998 as anything that relates to a living individual in which the individual can be identified:

- Directly from the information (e.g. name and address) or
- From the combination of this information with other information that may be readily accessible (e.g. address but not name), and
- Which affects the privacy of the subject, whether in personal, family, business or professional life

2.1.4 Sensitive personal data

Sensitive personal data is defined under the Data Protection Act 1998 as any 'personal data' relating to: racial or ethnic origin; political opinions; religious or similar beliefs; membership of a trade union; physical or mental health or condition; sexual life; the commission or alleged commission of any offence; any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

2.1.5 Information about someone who has died

The Data Protection Act 1998 does not apply to information about people who have died. However, such information may still be sensitive, confidential or relate to individuals who are still alive. Information about people who have died must still be shared under the provisions of this protocol.

2.1.6 De-personalised and aggregated information

Where de-personalised or aggregated information is no longer sensitive or identifiable, it may be shared outside of the scope of this protocol. However, where depersonalised or aggregated information may still be deemed sensitive (e.g. as a result of complexity, currency, potential for misinterpretation or misuse) it must still be treated with care under the provisions of this protocol.

2.1.7 Data in the public domain

This type of information incorporates any information, which is publicly available, where it relates to an individual or not.

2.2 Crime and Disorder Specific

2.2.1 Crime

A crime is defined as any act, default or conduct prejudicial to the community, the commission of which, by law, renders the person responsible liable to punishment by a fine, imprisonment, or other penalty.

2.2.2 Anti-Social Behaviour

Anti-social behaviour is defined as acting in a manner which causes, or is likely to cause, harassment, alarm or distress to one or more persons not of the same household.

2.2.3 Disorder

Disorder is considered to be the level or pattern of anti-social behaviour within a particular area.

3 THE LEGAL FRAMEWORK

The principal legislative instruments that control the exchange of information in the delivery of crime and disorder are:

- The Crime and Disorder Act 1998
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Common Law Duty of Confidence
- The Freedom of Information Act 2000
- Children Act 2004

Numerous other pieces of legislation place on public authorities a power or duty to share information in specific circumstances. All information sharing must be conducted in accordance with a relevant legal power or duty.

In particular, the Crime and Disorder Regulations 2007, Prescribed Information Regulations 2007 No. 1831, require statutory partners to share information that they hold in relation to a number of broad subject areas. While they relate to non-personal data, the regulations do now place a requirement on each responsible authority to share certain types of information with each other in a community safety context.

This information-sharing agreement recognises that the police are limited by the Management of Police Information Guidance (MOPI) to only share information for a defined policing purpose. These are protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice as well as any duty or responsibility arising from common or statute law.

More details about the legal and statutory framework is provided at Appendix B.

4 PARTIES TO THIS PROTOCOL

A full list of current signatories (including nominated designated officers) to this protocol can be found at Appendices C and D. This list will be updated at each annual review (normally in the summer of each year). Inbetween these annual revisions, an up to date list can be obtained from the CSP on 01344-352000 or e-mail: community.safety@bracknell-forest.gov.uk.

Each agency mentioned at Appendix C should sign a declaration under this protocol to ensure that exchanges fully comply with legal obligations covering personal information and certain types of anonymised information. The agreement should be signed by the chief officer or the data controller for that organisation as defined by the Data Protection Act.

All signatories must ensure that the protocol is fully implemented within their organisation and should develop procedures to ensure that all staff are aware of the issues around information sharing. They should also ensure that all information sharing leads and designated officers are conversant with this protocol and their responsibilities.

5 RESPONSIBILITIES

By signing up to this protocol, signatories are committed to a positive approach to information sharing. Signatories agree to meet the commitments and follow the processes outlined in this protocol in all instances of information sharing, including the following risk-assessment procedures:

- Confirm the identity of the person you are sharing with
- Obtain consent to share if safe, appropriate and feasible to do so
- Confirm the reason the information is required

- Be fully satisfied that it is necessary to share
- Check with a manager/specialist or seek legal advice if unsure
- Do not share more information than is necessary
- Inform the recipient if any of the information is potentially inaccurate or unreliable
- Ensure that the information is shared safely and securely
- Ensure that the information sharing is in accordance with the law
- Ensure that information is shared responsibly and in accordance with professional and ethical standards
- Be clear with the recipient how the information will be used
- Record what information is shared, when, with whom and why; and if you decide not to share, record your reason
- Consult with originating organisations before any information, received under this protocol, is used for any purpose other than that originally intended. This includes responding to requests for access to information from the public. Signatories are not obliged to consult where they are under a legal obligation to share information and any delays would result in serious harm. In such situations, signatories must inform the originating organisation as soon as is practicable.
- Appropriate staff training and awareness sessions are provided in relation to this protocol and the sharing of information
- Any electronic information is fully secure
- Arrangements are in place to test that this agreement, its associated working practices and legal requirements are being adhered to.

6 LIABILITY

6.1 Information Breaches

The Bracknell Forest CSP cannot be held responsible for breaches of this protocol or complaints arising from breaches.

Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants or agents.

Complaints and breaches must be dealt with by utilising signatories' own organisations' established policies and procedures for breaches and complaints made in relation to any legislation in connection with information exchange.

Any disclosure of information by an employee which is made in bad faith or for motives of personal gain will be the subject of an internal inquiry and be treated as a serious matter.

The disclosing agency is responsible for accuracy of the information and must inform the receiving agency of any subsequent changes to the information.

6.2 Indemnity

The members of the CSP, as receivers of information, will accept total liability for the loss or compromise of this information, as shared under this protocol, while it is under their custody or control.

Where a disclosing agency provides information to a requesting agency which is inaccurate and the requesting agency incurs liability, cost or expense as a result of its reliance upon the information provided, the disclosing agency shall indemnify the requesting agency against any such liability, cost or expense reasonably incurred.

This indemnity shall not apply:

- Where the liability arises from information supplied which is shown to have been incomplete or incorrect, where the requesting agency claiming the benefit of the indemnity have, in the application of the information supplied, been negligent in its use, whether through wilful wrongdoing, error or ineptitude
- Unless the agency claiming the benefit of this indemnity notifies the relevant agency as soon as possible of any action, claim or demand to which this indemnity applies, permits the relevant agency to deal with the action, claim or demand by settlement or otherwise and renders the authority all reasonable assistance in so dealing
- To the extent that the agency claiming the benefit of the indemnity makes any admission which may be prejudicial to the defence of the action, claim or demand

7 MANAGEMENT AND OPERATION OF THE PROTOCOL

7.1 Commencement and Review

This protocol is already active. Organisations already signed up to the protocol need not sign again after a revision. Where an organisation is an existing signatory to the protocol, but the signing Chief Executive or Director has left, the organisation will remain as a signatory. It is not expected that they resign, unless they wish to do so.

The review of this protocol will be completed annually and will be subject to approval by the signatories and the CSP.

The timetable may need to be adjusted in respect of significant legislative changes, the pressure of user feedback on processes or changes in context and circumstances.

It will be the responsibility of the Bracknell Forest CSP to initiate the review.

7.2 Governance and Scrutiny

The BFC Community Safety Team will provide ongoing advice and feedback on practical issues around the application of this protocol. At this team's discretion, minor changes, such as form design or clarification of guidance, will be made and posted on appropriate websites/circulated without the need for a full review process.

This team will be responsible for advice and updating all signatories on such changes and supplementary advice. More significant changes or changed demands or circumstances may require a full review.

The role of scrutiny will come from all partners signed up to this protocol.

8 INFORMATION SHARING IN PRACTICE: WHAT TO CONSIDER

8.1 What am I allowed to share legally?

All information must be shared in line with the law (see Appendix B). The following are alternative powers to share information, which should be considered:

Consent

Many of the data protection issues surrounding sharing information can be avoided if the subject (i.e. the person to whom the information relates) gives their permission to share the information with others. Careful consideration should be given before sharing the details of victims, witnesses or people who have made a complaint unless their permission has been gained in writing. This will apply even if they are not named but can be identified by inference.

Each individual agency should have a process for obtaining consent of the data subject to share information and these should be used when gaining consent to share where it is appropriate.

Where the data subject does not have capacity to give consent to share, consent may be sought from someone who may appropriately act on behalf of the data subject, for example an appropriate adult or someone who holds a relevant Power of Attorney.

If it is not possible or safe to obtain consent, consideration should be given to whether it is necessary to share without consent.

Recording and reviewing consent

A record should always be made of any consent that has been given or refused. This should be referred to when information is shared to ensure that the scope of the consent is not exceeded. Consent should be re-sought if the information is to be used for a different purpose to that recorded or if there has been an unreasonable lapse of time since consent to share was given.

Informed consent

Consent must always be informed. This means that the person giving consent must clearly understand all the available options and the consequences of them giving their consent.

Explicit or express consent

This is a clear and voluntary indication of consent to share specific information for one or more specified purposes.

Implied consent

This applies where it would be within the reasonable expectations of the data subject that information may be shared without needing to obtain explicit consent. It is likely to apply where information is routinely shared and the data subject is aware of this or where information sharing is intrinsic to the purpose for which the data subject supplied the information.

Withdrawal or reconfirmation of consent

The data subject may withdraw consent at any time and they should be made aware of this right. If consent is withdrawn, others with whom the information has been shared must be notified. Consent must not be assumed to be open-ended. Confirmation of continued consent should be sought after a reasonable time according to individual circumstances and an expiry date for consent should be recorded. In the event of a change in either the extent of information being sought or the need to share with agencies not included in the original consent agreement, a revised consent should be sought unless the information may legitimately be shared without consent.

8.2 What if I don't have the consent of the data subject?

It is not always safe, appropriate or feasible to obtain consent to share information. Circumstances where it may not be possible to obtain consent include:

- Where obtaining consent might be contrary to the public interest
- The data subject may be absent or not contactable
- The data subject may be permanently or temporarily incapacitated and has no appropriate representative
- The data subject has withheld or withdrawn their consent.

Under the Common Law Duty of Confidence, the Data Protection Act 1998 and the Human Rights Act 1998, it is possible to disclose information without consent in the cases of serious public interest or in the best interests of an individual. Decisions regarding the disclosure of information without consent must be made on a case-by-case basis and brought to the full attention of the designated officer of the organisation who is sharing the information. Any disclosure must always be proportionate and the minimum necessary to achieve the necessary objective.

If it is not possible to obtain consent before sharing information, the data subject should be informed as soon as possible after the information has been shared, unless this would be

inappropriate. The principle of sharing only that information which is proportionate and necessary should be considered at all times.

Best interests

Where an individual is unavailable or does not have capacity to consent to the sharing of information, a decision should be made in the best interests of that individual.

The impact of sharing or withholding information

Essentially, a decision to share information without consent rests on an assessment of the relative risk of disclosure and non-disclosure and a professional judgment on the most appropriate action that should be taken in the light of this assessment. Two key questions are:

- What if this information is not shared?; and
- Who will be affected by this information being shared?

The former considers whether a negative impact is likely if the information is withheld. There will be a clear interest in disclosing information where there is an evident risk to the life or well-being of an individual which is accentuated or not addressed by not doing so; the protection of health, morals and the rights and freedoms of others; public safety; and the prevention of crime and disorder. If substantive, the public interest value may over-ride that of an individual's human rights. The latter considers whether there is a disproportionately negative impact in information being made available, for example familial breakdown or personal risk resulting from unnecessary disclosure. Disclosure should be assessed for its potential impact on others who may be identifiable from the data (such as witnesses or staff who are involved in cases) or whose vulnerability makes their interests the over-riding consideration (such as children at risk).

Data Protection Exemptions

The Data Protection Act 1998 contains a number of exemptions whereby you may be able to share personal information without the data subject's consent. You may share information in these circumstances but you should assess each case individually. If a Data Protection exemption is valid and used, you must only give out information that is necessary for a purpose that is consistent with the exemptions you are using. You may not share irrelevant or additional information without receiving a specific request. The Information Commissioner also advises that you should decide whether failing to share information where an exemption

might apply would prejudice the purpose for which it has been requested (for example preventing crime and disorder). If you decide not to share the information, there would need to be a substantial chance rather than a slight risk that the purpose would be affected. It should also be stressed that these exemptions also apply to organisations outside the public sector. If an exemption applies, you must make sure that you follow the relevant principles and that processing still meets the other appropriate Data Protection principles. Each organisation will have their own processes for requesting exemptions. You can find more information about exemptions under the Data Protection Act that are relevant to these guidelines at http://www.opsi.gov.uk/acts/acts1998/ukdpa_19980029_en_1.

Public Interest

If a person who is the subject of consideration has not given their permission for their information to be shared, you must consider if there is a more important matter of public interest or justification for sharing the information. In making this decision you should consider the following questions:

- Do you need to share the information to prevent or detect crime, prevent disorder, protect public safety, or protect the rights and freedoms of others?
- Do you need to share the information to protect young or other vulnerable people?
- How does this person put others at risk?
- How vulnerable are those people who are at risk?
- How will the offender be affected by you sharing their information?
- Is the sharing of information proportionate to the intended aim?
- Is there an equally effective but less intrusive way of achieving that aim? Specific measures to prevent crime, reduce the fear of crime, detect crime, protect vulnerable people, maintain public safety or stop young offenders from re-offending are clearly in the public interest.

8.3 What about sensitive personal information?

When processing sensitive personal information (as defined earlier) you need to meet a condition from Schedule 2 and at least one from Schedule 3 of the Data Protection Act. You can find these at http://www.opsi.gov.uk/acts/acts1998/ukdpa_19980029_en_1. Where appropriate and possible, you should get permission to share information from the person who is the subject. They must give their permission freely, after you have told them what will happen when you share the information. If the person involved refuses to give you permission

but it is in the public's interest to share their information, you may be able to share it anyway. However, you should consider the following issues:

- Is the sharing of information proportionate to the intended aim?
- How vulnerable are those people who are at risk?
- How will the offender be affected by you sharing the information?
- Is there another equally effective way of achieving the same aim?
- Do you need to share the information to prevent or detect crime and uphold the rights and freedoms of the public?
- Do you need to share the information to protect other people? You should only share sensitive personal information that is needed to achieve the specific purpose. Where Designated Officers or similar exist within an organisation, a Designated Officer must make sure that the information is accurate and relevant to an enquiry before it is released.

8.4 What about de-personalised information?

The following guidance must be followed in relation to depersonalised information:

- Any agency or individual handling depersonalised information may not use that information to try to identify any individual.
- Information must not be released to those who have a commercial interest in its use
- Arrangements must be made for the secure storage of all depersonalised information
- Information must be destroyed when it is no longer required or in line with agencies' policies for managing records.

8.5 What if I want information from another agency?

Where designated officers or similar exist within an organisation, you must make the request through the designated officer of the agency from whom you are requesting the information.

8.6 What if a designated officer asks me for information?

When considering whether to share information in response to a request from a Designated Officer from another organisation, you must ask yourself:

- Do I have a legal power to share this information?

- If so, will I do so properly by following the law? This must include consideration of both common and statute law.
- Would it be in the public's interest to share the information? When considering whether to share information in response to a request from another organisation, you must consider the Simple Guide to Sharing Information (Appendix A)
- Confirm the identity of the person you are sharing with
- Obtain consent to share if safe, appropriate and feasible to do so
- Confirm the reason the information is required
- Be fully satisfied that it is necessary to share
- Check with a manager/specialist or seek legal advice if you are unsure
- Do not share more information than is necessary
- Inform the recipient if any of the information is potentially inaccurate or unreliable
- Ensure that the information is shared safely and securely
- Be clear with the recipient how the information will be used
- Record what information is shared, when, with whom, and why; and if you decide to not share, record your reason. If you give information to another agency, that agency must store the information securely and destroy the information when it is no longer needed for the purpose for which it was provided. The main principle of these guidelines is that an agency will always own the personal information it gives to another member of the partnership. The identity of the original data owner must be recorded against the relevant information. Anyone who receives this information must get permission from the original data owner before passing it on to anyone else.

8.7 What if my organisation hasn't nominated designated officers?

If your organisation does not have a nominated Designated Officer, you can still share information in accordance with the protocol. However, where practicable, you should consult with information sharing leads or your organisation's Data Protection Officer when sharing information outside of multi-agency groups.

8.8 When should requests be dealt with?

All requests for information should be dealt with within 10 working days of the request. If the requesting agency has an urgent timescale that needs to be met, they should make this clear to the agency that holds the information.

8.9 What if a subject wants access to information that relates to them?

Individuals whose information is held within organisations have certain rights of access to it, regardless of the media in which the information may be retained. Individuals also have a right to complain if they believe that an organisation is not complying with the requirements of the Data Protection legislation. Under the terms of the Data Protection Act, any individual has the right to request access to information held about them and this would include information held for community safety purposes. An individual may make a 'Subject Access' request under the provisions of the Data Protection Act using the existing mechanisms and forms of each agency. It is the responsibility of individual organisations to ensure that an up-to-date procedure is in place to deal with requests for access to information. If you have any queries with regard to subject access, you should consult the data controller in your organisation.

9 INFORMATION SHARING IN PRACTICE: WHAT TO DO

Types of enquiry There are three principal types of enquiry:

9.1 Simple enquiry

These are restricted to the confirmation that information is available on a specific individual or issue. This process confirms that information is held, but does not involve any further exchange of detail. An agency, signed up to this protocol, enquires through a designated officer, verbally or in writing, whether another agency holds information on an individual. If the answer is no, then the agency should be informed. If another agency is being asked, then the same process is followed.

9.2 Complex Enquiry

If the answer is yes, and the agency wants more information, this process then becomes a Complex Enquiry, which is any exchange that involves the transfer of detail beyond that covered by the simple enquiry. To support the sharing of information, four forms have been devised. These can act as a template or a guide in relation to the type of information that should be recorded whenever personal information is being shared. However, their use is not mandatory. A suggested process for sharing information in a crime and disorder context is outlined below, but again this is merely intended as a guide. However, it is important that details of the exchange are documented in some way and the approach suggested below enables this to happen. When sharing information under specific pieces of legislation, for example the Children Act 2004, contact should be made with the individual whom you are sharing with or who is requesting the information, to clarify the specific requirements regarding documenting the exchange

Proposed data sharing process The requesting agency should complete **Form 1,** or **Form 3** if the consent of the individual has been obtained to release this information. Copies of these forms are found in Appendix E and the process is as follows:

- Once **Form 1** or Form 3 has been completed, this should be sent to a designated officer of the agency.
- If the information requested will not be released, reasons for this must be stated on the **Form 1** and a copy returned to the requesting agency.
- If the information requested is to be shared, it should be shared promptly by the most appropriate secure medium.
- In all cases the original **Form 1** or **Form 3** should be retained with a record of what information has been shared and with whom.

9.3 Enquiries in Multi-Agency Meetings

Proposed data sharing process

Information exchange will also take place in various multi-agency meetings e.g. ASB Working Group, DASC Working Group, IOM meetings etc. where relevant agencies that are brought together to deal quickly with community safety issues, which are caused by problem individuals, families and other community problems. Of necessity, this will often require the sharing of personal and/or other sensitive or confidential information. Where information needs to be shared in these forums, the same principles will apply (including where necessary, the completion of **Forms 1** or **3**). Each of these groups meet with a remit to consider specific individuals or groups of individuals with a view to assessing risk, developing a fuller shared understanding of relevant issues or developing effective responses and interventions. Information exchange in this context will usually, in the first instance, be oral but must still be governed by data protection and confidentiality principles. To this end such meetings should ensure that:

- Those attending have a legitimate reason to be part of the process, either as information sharers or decision makers.
- If necessary the agenda structure should enable attendance for part only of meetings where a number of cases may be reviewed but are not relevant to all
- The individuals under consideration should normally be made aware of this process and, where appropriate, should be invited to attend. There will be circumstances

however where it will not be appropriate for the individuals to be made aware of the process.

- Data protection and confidentiality principles should be confirmed at the beginning of each meeting. A signatory form (**Form 2)** should be signed by those attending and kept as part of the record of the meeting. A copy of Form 2 is also found in Appendix E.
- The meeting record and any associated paperwork will be managed in accordance with data security principles. Any information or records shared outside of the group should be suitably depersonalised, or appropriately targeted. All groups/for a must ensure that controls applied to agenda and minute documents as are as secure as those used for requesting and securing personal information, since these will often name the individuals being considered and contain elements of the information contributory to the decision making process. Records of meetings and personal information must be subject to the principles set out in this protocol, particularly in relation to purpose and retention. These groups/fora may wish to identify a suitable designated officer who can act as a data and record manager on behalf of the group and ensure that information is kept securely and no longer than necessary.

Exceptional and emergency exchange

There will occasionally be circumstances in which information is required urgently and the form based exchange process cannot be followed. In these circumstances, the phone or face to face procedure must be followed, namely:

- Confirm the name, job title, department and organisation of the person asking for the information
- Confirm the reason for the information request, if appropriate
- Take a contact point, preferably main switchboard number or email address
- Check whether you can provide the information. If in doubt, tell the person you will come back to them when you know.
- Only give information to the person that has asked for it
- Make sure that you record:
  - Your name
  - The date
  - The reason you shared the information
  - Who authorised it
  - The name, job title, organisation and phone number of the person requesting the information.

Any exchange made under this provision MUST be backed up by paper exchange using the appropriate **Form (1 or 3)** no later than five days after the original exchange took place.

Secondary or Further Exchanges of Information

In the context of community safety partnership work, this protocol allows the secondary or further exchange of personal information with another agency, where the following conditions are met:

- the exchange is authorised in writing by a Designated Officer of the agency, which originally held the information;
- the exchange would allow the person receiving the information to carry out their clearly defined role in the Community Safety Plan;
- the public interest is more important than confidentiality;
- the information is processed fairly and lawfully; and
- the third agency is a signatory to this protocol or can prove that they are signed up to an equivalent agreement.

What happens if the information changes or is wrong?

You may need to correct or update information that you have supplied in response to a request for information. This may be as a result of inaccuracies uncovered, updated relevant information or an authorised correction requested by the subject. You must ensure that any additional or corrected information remains appropriate in respect of the original application and agreement to exchange. Do not provide any information that goes beyond the original request without a new form (Form 4) being submitted by the requester and approved by the information holder. A copy of this form is found in Appendix E. If you discover that any information you have received is not accurate or is unsuitable for the purpose, you should inform the information owner as soon as possible. The information owner will be responsible for correcting the information and advising everyone else who received it of the necessary corrections. Any amendments should be made using Form 4.

The Data Protection Act principles require that data is exchanged, held and disposed of within an effective security framework. The following are a set of general principles relating to sensitive, personal and sensitive personal data:

- At all stages of the exchange, the principle that the information should be available only to those who have a specific and legitimate need to see it must be maintained by both the sender and the recipient.
- Documents and information exchanged should be protectively marked where a scheme has been adopted by an organisation. This is to ensure that the person receiving the information can adopt suitable security measures to prevent the information from being compromised or unlawfully disclosed.
- Data must only be sent if the means of transmission is secure (See 'How can I exchange information securely?' below) and it can be established that the appropriate recipient's access to the transmission is equally secure.
- Data must be stored securely, regularly reviewed and disposed of in accordance with the receiving organisations retention and disposal policy and procedures when no longer required for the purpose it was originally obtained.
- This protocol is based on the principle that sharing of personal data between agencies is done on an individual case-by-case basis. Occasionally, however, it may be necessary for organisations or agencies to transfer data in bulk or in batches e.g. personal data referring to 20 or more individuals. To ensure the security of this data, controls must be in place to secure the data during transit and when received. Such transfers must be compliant with the sending organisation's security policy or guidance and agreed by the receiving organisation whether paper documents or records or electronic data (e.g. encryption of all personal identifiable data held on portable media such as, laptops, CDs, DVDs, memory sticks or pen drives, tapes, etc).

How can I exchange information securely?

It is important that information is shared safely and only shared with the intended recipient. The information should show the originator's details, including organisation name (if applicable) and date. Information can be shared in a variety of ways and there are advantages and disadvantages to each method. Always choose the most secure and confidential method that is available to you - think through all these methods before you use one. The ways in which you may choose to exchange information are set out below:

E-mail

Please note that e-mail is only secure if the e-mail system itself is secure. Encryption and password protection do not provide sufficient security to exchange personal and sensitive

information using normal e-mail systems. Note: some organisations may not allow encrypted Information Sharing in Practice: Keeping information secure

Fax

This is only secure if the person who wants the information is waiting at the machine to receive the document immediately. Do not assume this will always be the case and ensure they are waiting for your fax before it is sent. It is recommended that a cover sheet is transmitted first with the information itself sent only after a confirming response has been received.

Postal or Courier Services

Postal Services can never be fully secure and are not recommended unless fax or secure e-mail is not possible. If you have to use post, ensure that you use an envelope that will show if it has been tampered with (preferably inside another envelope), and is marked 'Private and confidential addressee only'. It is recommended that if the Post Office system is used, Recorded Delivery or Registered Delivery is chosen, as this allows the mail to be tracked. A courier service could alternatively be used, depending on the sender's requirements or sensitivity of the information.

Personal exchange

Paper copies of information can be exchanged in person provided that both the information holder and the recipient take appropriate measures to ensure that they cannot be read by anyone who does not have a legitimate reason to do so. Paper copies should be kept secure at all times.

Verbal Exchange

This is only secure if it is not repeated to anyone who is not authorised to hear it, or overheard when exchanged or discussed (e.g. in a busy office or during a conference phone call). If information is exchanged verbally in a manner where it is not recorded at the time, the exchange should be validated and confirmed in writing as soon as possible.

Verbal information should be subject to the same considerations as written, and should not be exchanged unless both parties are satisfied that the request is legitimate and there is a good reason for not pursuing a written route

Be extremely careful when you share information verbally. Ideally you should do this in a conference-style meeting with full minutes where the exchange can be recorded and validated.

However information is shared, ensure that it is appropriate within the protocol's guidance, do not repeat or share it casually, and take responsibility for it.

Conference

Much information sharing will take place in confidential conference meetings to determine a course of action in respect of specific named individuals and to which appropriate individuals are invited. Exchange may be oral or on paper but data protection principles must still apply with attendees only being present where it is appropriate for them to share the information.

How can I Protectively Mark Information Assets?

An established framework for document security marking should be adopted on all information to be exchanged as required by ISO /IEC 17799 or ISO /IEC 27001 Standards.

Frameworks exist in most sectors and most organisations use terms such as "Internal only" or "Confidential" and, as a general principle, all personal information should carry a protective marking, or the equivalent for their organisation.

Any use of protective marking on documents should make a distinction between the categories that are used to protect sensitive internal business information and those used to protect personal data. This distinction may affect the extent to which similarly marked documents may be shared, even if there is no personal data included. It is important that any receiving organisation or agency is made aware of what the protective marking means so that the appropriate protective security measures can be applied to the information assets shared.

As an example, some police forces use the Government Protective Marking Scheme, which has six levels of Protective Marking (shown below). These protective markings are underpinned by the principle that information is only made available with a legitimate "need to know" and as such any protectively marked documents should not be disclosed further without the consent of the originator.

The originator of the asset (that is all material assets, i.e. papers, drawings, images, disks and all forms of electronic data records) indicates to others the levels of protection required when handling the asset in question, in terms of its sensitivity, security, storage, movement both within and outside the originator's own department or organisation and its ultimate method of disposal. Be aware that applying too high a protective marking to information can inhibit access; lead to unnecessary protective controls and impair operational efficiency. Conversely, applying too low a protective marking can put information at risk of compromise, since appropriate security controls may not be in place.

The following protective markings are given as an example:

• NOT PROTECTIVELY MARKED
• PROTECT
• RESTRICTED
• CONFIDENTIAL
• SECRET
• TOP SECRET

Although these markings may be applied by the Police to their own documents, it is not a requirement that non-Police organisations apply the same classification criteria when marking their own documents. The methods of secure data storage and data disposal below are adequate for the secure handling of protectively marked assets at NOT PROTECTIVELY MARKED, PROTECT, RESTRICTED and CONFIDENTIAL. It is unlikely that Secret or Top Secret documents will require sharing under the terms of this protocol. NOT PROTECTIVELY MARKED may be used to indicate positively that a protective marking is not needed.

PROTECT relates to information which may:

• cause distress to individuals;
• breach proper undertakings to maintain the confidence of information provided by third parties;
• breach statutory restrictions on the disclosure of information
• cause financial loss or loss of earning potential, or to facilitate improper gain; unfair advantage for individuals or companies;
• prejudice the investigation or facilitate the commission of crime;

RESTRICTED relates to information which may:

• cause substantial distress to individuals;
• cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies;
• prejudice the investigation or facilitate the commission of crime;
• breach proper undertakings to maintain the confidence of information provided by third parties;
• breach statutory restrictions on disclosure of information;
• undermine the proper management of the public sector and its operations.

CONFIDENTIAL relates to information which may:

• prejudice individual security or liberty;
• cause damage to the operational effectiveness or security of United Kingdom or allied forces or the effectiveness of valuable security or intelligence operations;
• work substantially against national finances or economic and commercial interests;
• substantially to undermine the financial viability of major organisations;
• impede the investigation or facilitate the commission of serious crime;
• shut down or otherwise substantially disrupt significant national operations.

How can I store the information securely?

Once information has been shared, it must be stored securely.

• Manual (non-electronic) information should be:
    - o Dated, filed and marked in accordance with protective marking principles or with the receiving agency's procedures.
    - o Linked to any records of the exchange to ensure that the original purpose remains the basis for review and disposal.
    - o Kept in a secure lockable filing cabinet when not in use.
    - o Kept away from wider view when being used.
    - o Regularly reviewed and disposed of when no longer appropriate to be kept or in accordance with an organisation's retention or disposal policy and procedures.

• Electronic information should be:
    - o Flagged in accordance with protective marking principles.
    - o Password protected or encrypted, with passwords regularly changed.
    - o Stored on a secure drive or server with restricted access.
    - o Protected by a security screensaver, if left open but unused.

- o Linked to any records of the exchange to ensure that the original purpose remains the basis for review and disposal.
- o Regularly reviewed and deleted (locally and on any back-ups) when no longer appropriate to be kept.

How do I dispose of the data?

The length of time that exchanged information is retained will need to be determined on a case by case basis but always in compliance with the requirement that it is only kept for the minimum period necessary to achieve the specific aims for which it was obtained. After this, the information must be returned to the owner or destroyed, as agreed. Both the requesting and the supplying agency should keep a copy of any records relating to information exchanged for at least two years. Each Designated Officer, or similar, is responsible for reviewing the information they hold on a regular basis. Physical copies of information should be shredded when they are no longer required; this includes any floppy disks, compact disks or DVDs. Electronic copies should be “double deleted” i.e. not just from the disk or server, but also from any back-ups that are retained. Where information is shared in a meeting, once the issue to which that issue relates has been dealt with, the meeting may take the decision to dispose of the information. This decision needs to be reflected in the minutes of the meeting.

10 CLOSURE/TERMINATION OF AGREEMENT

Any party can suspend their participation in this protocol in the event of a serious security breach. Following any suspension, an enquiry must be held by a panel made up from signatories to this protocol or their nominated representative. This enquiry shall take place within 14 days of such suspension.

Termination/suspension of this protocol shall be notified in writing to all other parties to the protocol as soon as possible.

11 DECLARATION AND SIGNATURE

DECLARATION

I,…… hereby sign the Bracknell Forest Community Safety Partnership (CSP) Information and Data Sharing Protocol and agree to abide by the terms and conditions contained therein.

Role/Designation

Appendix A

Simple Guide to Information Sharing

- Confirm the identity of the person you are sharing with
- Obtain consent to share if safe, appropriate and feasible to do so
- Confirm the reason the information is required

- Be fully satisfied that it is necessary to share
- Check with a manager/specialist or seek legal advice if you are unsure
- Do not share more information than is necessary
- Inform the recipient if any of the information is potentially inaccurate or unreliable
- Ensure that the information is shared safely and securely
- Be clear with the recipient how the information will be used
- Record with information is shared, when, with whom, and why; and if you decide to not share, record your reason

Appendix B

The Legal Framework

Before the sharing of information takes place, it must first be determined whether a legal basis exists for that information sharing. The agency that is to receive the information must identify the legal power that allows them to lawfully request the information. The majority of requests for information exchange within the remit of the CSP will be under one of the following areas of legislation:

Section 115 of the Crime & Disorder Act 1998

Where certain conditions are satisfied, Section 115 enables disclosure of information for the purposes of any provision of the Crime and Disorder Act 1998 (or any amendment to that legislation) to a relevant authority, or to a person acting on behalf of such an authority. The full document can be viewed at:
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980037_en_1.htm

Home Office Review of the Partnership Provisions of the Crime and Disorder Act 1998 – Report of Findings (January 2006)

Paragraph 3.16 of this document states that '***we intend to strengthen section 115 of the Crime and Disorder Act, which gives relevant agencies the power to disclose information, and place a duty on responsible authorities to share depersonalised data which are relevant for community safety purposes and already held in a depersonalised format. This duty will apply to data already collected by partner agencies in a depersonalised format.'***

In addition, Paragraph 3.17 states that '***it is vital for every CDRP/CSP to have an information-sharing protocol in place which formally sets out the principles of the partnership's data sharing arrangements, detailing what will be exchanged, by whom, with whom, for what purposes and with which safeguards in place.'***

Statutory Instrument 2007 No. 1830 Crime & Disorder (Formulation and Implementation of Strategy) Regulations 2007 – Home Office

Section 4 (1) of the Crime & Disorder (Formulation and Implementation of Strategy) Regulations 2007 (which sets out the formation of a Strategy Group within each CSP as at 1 August 2007), states that '***the strategy group shall have in place arrangements for the sharing of information between responsible authorities and shall prepare a protocol setting out those arrangements.'*** The full document can be viewed at:
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20071830_en.pdf

Management of Police Information (MoPI) Guidance (2nd Edition: 2010)

Compliance of this protocol against the above guidance has been verified. The guidance document describes policing purposes relating to information management and is designed to provide a common national framework for the management of police information, highlighting the importance of common standards in high risk areas of activity.
The full document can be viewed at:
http://www.npia.police.uk/en/docs/MoPI_refreshed_Guidance.pdf

Note:

Where the police are requested to share information with a partner and a statutory obligation or power does not exist, a policing purpose must be established as the decision to share is risk-based and must take into account the source of the information and any restriction on its dissemination.

Data Protection Act 1998

Section 29 of this Act allows for the exchange of information where it is for the purposes of the prevention or detection of crime, apprehension or prosecution of offenders and where failure to disclose would be likely to prejudice those objectives. The full document can be viewed at: http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Freedom of Information Act 2000

Each party to the protocol shall, where practical, publish this protocol on its website and refer to it where relevant. If a party wishes to withhold all or part of the protocol from publication, it shall inform the other parties as soon as reasonably possible and a collective decision, as to whether this information should be withheld or not, shall be made. Information shall only be withheld where, should an application for that information be made under FOIA 2000, it is likely that the information would be exempt from disclosure and the public interest lies in favour of withholding. However, nothing in this paragraph shall prevent the individual parties from exercising its obligations and responsibilities under FOIA 2000. This guidance can be found at: http://www.legislation.gov.uk/ukpga/2000/36/contents

Human Rights Act 1998

Article 8 of this Act may impact on information sharing as it states that everyone has the right to respect for his/her private and family life, his/her home and correspondence. This right is not absolute – interference can be justified in the interests of the prevention of crime and disorder. The following principles should be considered:

- Is there a legal basis for the action being taken?
- Does it pursue a legitimate aim (as outlined in the particular Convention article)?
- Is the action taken proportionate and the least intrusive method of achieving that aim?

The full document can be viewed at:
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1

Appendix C

Parties to the Protocol

Thames Valley Police (Bracknell Local Police Area)
Thames Valley Police Authority
Bracknell Forest Borough Council (including the Youth Offending Service and Drug and Alcohol Action Team)
Bracknell Town Council
Crowthorne Parish Council
Sandhurst Town Council
Warfield Parish Council

Winkfield Parish Council
Thames Valley Probation
Royal Berkshire Fire & Rescue Service
SMART Criminal Justice Services (CJS)
CRI
Heatherwood and Wexham Park Hospitals NHS Foundation Trust
Frimley Park Hospital NHS Foundation Trust
South Central Ambulance Service NHS Trust
Jobcentre Plus
Berkshire Women's Aid (BWA)
Royal Military Academy Sandhurst
A2 Dominion Housing Group
Ability Housing Association
Bracknell Forest Homes
Dimensions (UK) Ltd
Home
Housing 21
The Guinness Trust
James Butcher Housing Association Ltd
London and Quadrant Housing Trust
Paradigm Housing Group Ltd
Sovereign Housing Association Ltd
Southern Housing
Thames Valley Housing Association
One Housing Group
Affinity Sutton Homes
Radian Housing Association

Appendix D

Designated Officers

Thames Valley Police (Local Police Area: Bracknell Forest)

Designated officer:	**Local Police Area Commander (or as delegated)**
Postal address:	**Bracknell Police Station** **The Broadway** **Bracknell** **RG12 1AD**
Contact e-mail:	**simon.bowden@thamesvalley.pnn.police.uk**
Contact telephone number:	**01344 823410**

Thames Valley Police Authority

Designated officer:	**Solicitor (or as delegated)**
Postal address:	**The Farmhouse**
	Oxford Road
	Kidlington
	OX5 2NX
Contact e-mail:	**paul.thomas@thamesvalley.pnn.police.uk**
Contact telephone number:	**01865 846780**

Bracknell Forest Borough Council

Designated officer:	**Chief Executive (or as delegated)**
Postal address:	**Easthampstead House**
	Town Square
	Bracknell
	RG12 1AQ
Contact e-mail:	**chief.executive@bracknell-forest.gov.uk**
Contact telephone number:	**01344 352000**

Including:

Youth Offending Service (YOS)

Designated officer:	**Head of YOS**
Postal address:	**76 Binfield Road**
	Bracknell
	RG42 2AR
Contact e-mail:	**youth.offending-team@bracknell-forest.gov.uk**
Contact telephone number:	**01344 354300**

and

Drug and Alcohol Action Team (DAAT)

Designated officer:	**DAAT Manager**
Postal address:	**New Hope** **92 Broadway** **Bracknell** **RG12 1AR**
Contact e-mail:	**drug.actionteam@bracknell-forest.gov.uk**
Contact telephone number:	**01344 312360**

Bracknell Town Council

Designated officer:	**Town Clerk (or as delegated)**
Postal address:	**Bracknell Town Council** **Brooke House** **High Street** **Bracknell** **RG12 1LL**
Contact e-mail:	**clerk@bracknelltowncouncil.gov.uk**
Contact telephone number:	**01344 420079**

Crowthorne Parish Council

Designated officer:	**Clerk (or as delegated)**
Postal address:	**Crowthorne Parish Council** **Parish Office** **Morgan Centre** **Wellington Road** **Crowthorne** **RG45 7LD**
Contact e-mail:	**clerk@crowthornepc.org.uk**
Contact telephone number:	**01344 771251**

Sandhurst Town Council

Designated officer:	**Executive Officer (or as delegated)**
Postal address:	**Sandhurst Town Council**

	Council Offices
	Sandhurst Memorial Park
	Yorktown Road
	Sandhurst
	GU47 9BJ
Contact e-mail:	**stc@sandhurst.gov.uk**
Contact telephone number:	**01252 879060**

Warfield Parish Council

Designated officer:	**Clerk (or as delegated)**
Postal address:	**Warfield Parish Council**
	17 Country Lane
	Warfield
	RG42 3JP
Contact e-mail:	**clerk@warfieldparishcouncil.org.uk**
Contact telephone number:	**01344 457777**

Winkfield Parish Council

Designated officer:	**Clerk (or as delegated)**
Postal address:	**Winkfield Parish Council**
	Council Offices
	Fernbank Road
	Ascot
	SL5 8JW
Contact e-mail:	**info@winkfieldparishcouncil.org.uk**
Contact telephone number:	**01344 885110**

Thames Valley Probation Area

Designated officer:	**Director (or as delegated)**
Postal address:	**Revelstoke House**
	Chalvey Park
	Slough
	SL1 2HF

Contact e-mail:	**graham.mccartney@thames-valley.probation.gsi.gov.uk**
Contact telephone number:	**01869 255300**

Royal Berkshire Fire & Rescue Service (RBFRS)

Designated officer:	**Fire Officer (or as delegated)**
Postal address:	**Headquarters** **103 Dee Road** **Tilehurst** **Reading** **RG30 4FS**
Contact e-mail:	**jacquesp@rbfrs.co.uk**
Contact telephone number:	**01189 322477**

SMART Criminal Justice Services (CJS)

Designated officer:	**Service Manager**
Postal address:	**SMART** **c/o New Hope Substance Misuse Centre** **92 The Broadway** **Bracknell** **RG12 1AR**
Contact e-mail:	**pcarvell@smartcjs.org.uk**
Contact telephone number:	**01344 312360**

CRI

Designated officer:	**Project Manager (Reading Dais)**
Postal address:	**79 London Street** **Reading** **RG1 4QA**
Contact e-mail:	**zoe.rice@cri.org.uk**
Contact telephone number:	**0118 9567441**

Heatherwood and Wexham Park Hospitals NHS Foundation Trust

Designated officer:	**Chief Executive (or as delegated)**
Postal address:	**Wexham Park Hospital**
	Slough
	SL2 4HL
Contact e-mail:	**ian.collyer@hwph-tr.nhs.uk**
Contact telephone number:	**01753 633585**

Frimley Park Hospital NHS Foundation Trust

Designated officer:	**Information Governance Manager (or as delegated)**
Postal address:	**Portsmouth Road**
	Frimley
	GU16 7UJ
Contact e-mail:	**information.governance@fph-tr.nhs.uk**
Contact telephone number:	**01276 604 675**

South Central Ambulance Service NHS Trust

Designated officer:	**Information Governance Manager (or as delegated)**
Postal address:	**Units 7-8 Talisman Business Park**
	Talisman Road
	Bicester
	OX26 6HR
Contact e-mail:	**barbara.sansom@scas.nhs.uk**
Contact telephone number:	**01869 365000**

Jobcentre Plus

Designated officer:	**Thames Valley District Drugs Coordinator**
Postal address:	**Fitzwilliam House**
	Skimped Hill Lane
	Bracknell
	RG12 1JX
Contact e-mail:	**contact-us@jobcentreplus.gsi.gov.uk**
Contact telephone number:	**0845 6043719**

Berkshire Women's Aid (BWA)

Designated officer:	**Chief Executive Officer (or as delegated)**
Postal address:	**P O Box 413**
	Reading
	RG1 8XL
Contact e-mail:	**ceo@bwaid.org.uk**
Contact telephone number:	**0118 950 4003**

The Royal Military Academy

Designated officer:	**Unit Security Officer**
Postal address:	**Sandhurst**
	Camberley
	GU14 4PQ
Contact e-mail:	**RMAS-SSU-2IC@mod.uk**
Contact telephone number:	**01276 412179**

A2 Dominion Housing Group

Designated officer:	**Joanne Carter**
Postal address:	**Spelthorne House**
	Thames Street
	Staines
	TW18 4TA
Contact e-mail:	**joanne.carter@a2dominion.co.uk**
Contact telephone number:	**0208 825 1727**

Ability Housing Association

Designated officer:	**Chief Executive (or as delegated)**
Postal address:	**2 Burlington Court**
	Burlington Road
	Slough
	SL1 2J
Contact e-mail:	**info@ability-housing.co.uk**
Contact telephone number:	**01753 571324**

Bracknell Forest Homes

Designated officer:	**Chief Executive (or as delegated)**
Postal address:	**Berkshire Court**
	Western Road
	Bracknell
	Berkshire
	RG12 1RE
Contact e-mail:	**bfh@bracknellforesthomes.org.uk**
Contact telephone number:	**0800 692 3000**

Dimensions (UK) Ltd

Designated Officer:	**Chief Officer (or as delegated)**
Postal address:	**Bracknell Regional Office**
	67 Broadway
	Bracknell
	RG12 1BB
Contact e-mail:	**info@dimensions-uk.org**
Contact telephone number:	**0845 160 2230**

Home

Designated Officer:	**Chief Executive (or as delegated)**
Postal address:	**Maxwell Hart Building**
	612 Reading Road
	Winnersh
	RG41 5HF
Contact e-mail:	**home-reading@homegroup.org.uk**
Contact telephone number:	**0118 9777600**

Housing 21

Designated officer:	**Chief Executive (or as delegated)**
Postal Address:	**Long Wood House**
	Love Lane
	Cirencester
	GL7 1YG
Contact e-mail:	**enquiries@housing21.co.uk**
Contact telephone number:	**0345 607 0272**

The Guinness Trust

Designated officer:	**Chief Executive (or as delegated)**
Postal address:	**Boyd Court**
	Downshire Way
	Bracknell
	RG42 1PY
Contact e-mail:	**david.allen@guinness.org.uk**
Contact telephone number:	**01344 485122**

James Butcher Housing Association Ltd

Designated officer:	**Chief Executive (or as delegated)**

Postal address:	**39 High Street**
	Theale
	Reading
	Berkshire
	RG7 5AH
Contact e-mail:	**service.centre@shgroup.org.uk**
Contact telephone number:	**08456 120 021**

London & Quadrant Housing Trust

Designated officer:	**Chief Executive (or as delegated: David Montague)**
Postal address:	**Beacon House**
	50 Stoke Road
	Slough
	SL2 5AW
Contact e-mail:	**lqdirect@lqgroup.org.uk**
Contact telephone number:	**0800 015 6536**

Paradigm Housing Group Ltd

Designated officer:	**Chief Executive (or as delegated)**
Postal address:	**Hundreds House**
	24 London Road West
	Amersham
	HP7 0EZ
Contact e-mail:	**enquiries@paradigmhousing.co.uk**
Contact telephone number:	**01494 830991**

Sovereign Housing Association Ltd

Designated officer:	**ASB Advisor**
Postal address:	**Sovereign South and West**

	Berkshire House
	22-24 Bartholomew Street
	Newbury
	RG14 5LL
Contact e-mail:	**rebecca.horne@sovereign.org.uk**
Contact telephone number:	**01635 572166**

Southern Housing Group

Designated officer:	**Colin Waters**
Postal address:	**Southern Housing Group** **Fleet House** **59 - 61 Clerkenwell Road** **London** **EC1M 5LA**
Contact e-mail:	**service.centre@shgroup.org.uk**
Contact telephone number:	**08456 120 021**

Thames Valley Housing Association

Designated officer:	**Chief Executive (or as delegated)**
Postal address:	**Premier House**
	52 London Road
	Twickenham
	TW1 3RP
Contact e-mail:	**info@tvha.co.uk**
Contact telephone number:	**020 8607 0607**

One Housing Group

Designated officer:	**Chief Executive (or as delegated)**
Postal address:	**Ground Floor**

	25-27 Broadway
	Maidenhead
	SL4 1LY
Contact e-mail:	**sneedham@onehousinggroup.co.uk**
Contact telephone number:	**020 8821 5330**

Affinity Sutton Homes

Designated officer:	**Chief Executive (or as delegated)**
Postal address:	**12 Elstree Way**
	Borehamwood
	Hertfordshire
	WD6 1JE
Contact e-mail:	**natasha.greenwood@williamsutton.org.uk**
Contact telephone number:	**020 8235 7000**

Radian Group Ltd

Designated officer:	**Community Safety Officer**
Postal address:	**Parkside House**
	33-39 Sheet Street
	Windsor
	SL4 1BY
Contact e-mail:	**steven.knowles@radian.co.uk**
Contact telephone number:	**01753 747392**

Appendix E

CONFIDENTIAL

Sample Form 1: Request for Personal Information

Form for requesting personal or sensitive personal information from another agency.

Part 1: to be completed by the agency requesting information

Personal details of the subject of the information [Only include enough detail as is necessary for the recipient to identify the subject]			
Our reference:		Surname:	
Forenames:		Any previous surnames:	
Also known as:		Date and place of birth:	
Current address: Postcode:		Previous address: (if known)	
Scope and reason for the request			
Information required:			
Data Protection Act justification for disclosing this information:			
Purpose for which this information is required:			
Consequences of failure to provide information:			
Signed		Date	
Name		Job title	
Agency			

Part 2: to be completed by the agency that holds the information

Information supplied?		Yes / No [delete as applicable]	
If no, reason for refusal:			
Signed		Date	
Name		Job title	
Agency			

We, the signatories, understand, that this request for information has been made according to the principles of the ISP and that the information shared as a result is for the specific purpose stated.

Under the principles of the ISP, both the requesting and the supplying agency should keep a copy of any records relating to information exchanged in line with their organisation's policies, but for at least two years.

CONFIDENTIAL

Sample Form 2: Information Sharing in Multi-Agency Meetings

Declaration of agreement to information sharing principles for use in confidential meetings	
Meeting title:	
Purpose of meeting:	
Date:	

We, the undersigned, accept and understand that the principles of the Surrey Multi-Agency Information Sharing Protocol and the legislation regulating the exchange of information apply to the content of this meeting. We understand that information shared and exchanged at this meeting is for the specific purpose identified above.

Name	Organisation	Signature

1. Those attending have a legitimate reason to be part of the process, either as information sharers or decision makers.
2. If necessary the agenda structure should enable attendance for part only of meetings where a number of cases may be reviewed but are not relevant to all.
3. The individuals under consideration should normally be made aware of this process and, where appropriate, should be invited to attend. However, in some circumstances where it will not be appropriate for the individuals to be made aware of the process.
4. Data protection and confidentiality principles should be confirmed at the beginning of each meeting.

This form will be retained as part of the meeting record. Please file this form with a copy of all information shared attached to it. Under the principles of the ISP each agency should keep a copy of any records relating to information shared in line with their organisation's policies, but for at least two years.

CONFIDENTIAL

Sample Form 3: Permission to Share Personal and Confidential Information

Form to indicate consent to share personal and confidential information

Our reference	

1. Your details			
Your surname:			
Your forenames:			
Address including postcode:			
2. Who we are (Organisation and contact details)			
3. Your personal and confidential information that we wish to share			
4. The people with whom we want to share this information (please indicate if you do not want us to share with any of those listed)			
5. The reason we want to share it			
6. Declaration I give you permission to share my personal and confidential information as described in section 3, with the people indicated in section 4 and for the purpose described in section 5. I understand that I may withdraw my consent at any time at the address given in section 2.			
Signed		Date	
7. To be signed by the person requesting consent			
Signed		Date	
We will only use the information on this form for the purpose mentioned. We cannot use it for any other purpose, unless you have given us permission.			

This form will be filed with a copy of all information shared attached to it. In line with the principles of the ISP, each agency will keep a copy of any records relating to information shared in line with their organisation's policies, but for at least two years.

CONFIDENTIAL

Sample Form 4: Altering Information which has already been supplied

You must ensure that any additional or corrected information remains appropriate in respect of the original application and agreement to exchange. Do not use this form to provide additional information that goes beyond the scope of the original agreed information exchange.

Part 1: the information holder should complete this section

This information is being provided to:	Correct inaccurate information Update previous information
Reference:	Date:
Who is asking for this information to be amended?	

Details of person sending this amendment			
Name:		Position / Role:	
Organisation:		Telephone number:	
Address:		Email:	
Signature:		Date:	
Details of person receiving this amendment			
Name:		Position / Role:	
Organisation:		Telephone number:	
Address:		Email:	
Details of the data subject (the person the information is about)			
Name:		Date of birth:	
Address:			
Details of amendments to be made			

Part 2: the recipient should complete this section

Details of person making the amendment:			
Name:		Position / Role:	
Organisation:		Telephone number:	
Address:		Email:	
Date amendment was made:			
Signature:			

We, the signatories, understand, that this request for information has been made according to the principles of the ISP and that the information shared as a result is for the specific purpose stated.

Under the principles of the ISP, both the requesting and the supplying agency should keep a copy of any records relating to information exchanged in line with their organisation's policies, but for at least two years.