Surrey Crime & Disorder

Information Sharing Protocol

Contact: Louise Gibbins
Community Safety Officer, Surrey County Council
Louise.gibbins@surreycc.gov.uk

Contents

1. Introduction

Confident and timely information exchange is the key to multi agency crime reduction work. When conducted appropriately it reveals a more accurate picture of what is going on and enables more effective interventions for both perpetrators and victims.

The Surrey Crime & Disorder Information Sharing Protocol (C&D ISP) is a context specific, tier two protocol that is compliant with the overarching Surrey Multi Agency Information Sharing Protocol (MAISP).

The MAISP is the overarching protocol for all multi agency information sharing in Surrey. It provides a common set of principles and standards under which partner organisations will share information. It records the commitment of Senior Officers in each participating organisation to meet agreed standards for the sharing for personal identifiable information.

When sharing confidential information, agencies need to be clear about why and how this will happen. Many organisations have already established protocols for sharing information, sometimes in line with national standards or differing professional requirements. These organisation-specific protocols remain in force, with Surrey's overarching MAISP there to provide the ground rules for how they can operate together.

2. The Process for Crime & Disorder Information Sharing

Share with confidence and remember, it is appropriate to share where the disclosure is necessary for the:

- Prevention or detection of crime, disorder and anti social behaviour
- Protection of public safety
- Protection of the rights and freedoms of others
- Protection of young or other vulnerable people

Share with consent of the individual where appropriate and, where possible respect the wishes of those who do not consent for you to share their confidential information. The Surrey MAISP provides guidance on obtaining, recording and reviewing and consent. You may still share information without consent, if in your judgement, that lack of consent can be overridden in the public interest, for example:

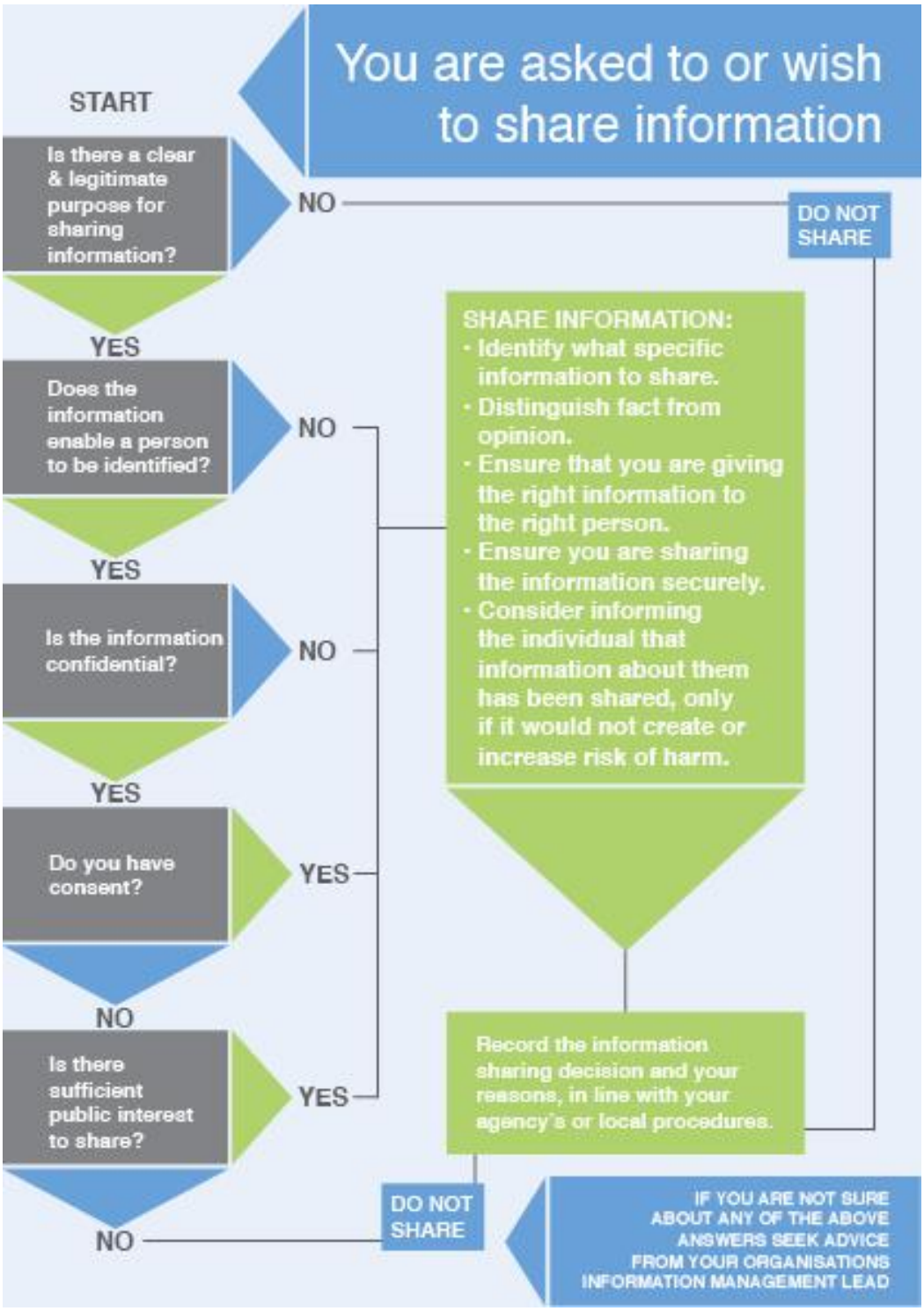
- Safeguarding children
- Protecting other vulnerable people
- Preventing the commission of criminal offences
- Bringing offenders to justice

Consider safety and well being. Base your information sharing decisions on considerations of the safety and well-being of the person and others (immediate family, wider community, national security) who may be affected.

Necessary, proportionate, relevant, accurate, timely and secure

Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely. Remember you do not need to share everything, always ensure that you know what specific information is required and why.

Keep a record of your decision and the reasons for it – whether it is to share information or not. The Surrey MAISP provides guidance and forms to assist you in requesting and processing requests for information.


You are asked to or wish to share information
START
Is there a clear & legitimate purpose for sharing information?
NO
DO NOT SHARE
YES
Does the information enable a person to be identified?
NO
YES
Is the information confidential?
NO
YES
Do you have consent?
YES
NO
Is there sufficient public interest to share?
YES
NO
SHARE INFORMATION:
· Identify what specific information to share.
· Distinguish fact from opinion.
· Ensure that you are giving the right information to the right person.
· Ensure you are sharing the information securely.
· Consider informing the individual that information about them has been shared, only if it would not create or increase risk of harm.
Record the information sharing decision and your reasons, in line with your agency's or local procedures.
DO NOT SHARE
IF YOU ARE NOT SURE ABOUT ANY OF THE ABOVE ANSWERS SEEK ADVICE FROM YOUR ORGANISATIONS INFORMATION MANAGEMENT LEAD

3. Scope

The C&D ISP is intended to facilitate the exchange of personal or sensitive information in any format (i.e. paper based, verbal, electronic) between signatories for the:

- Prevention or detection of crime, disorder and anti social behaviour
- Protection of public safety
- Protection of rights and freedoms of others
- Protection of young or other vulnerable people

The C&D ISP must be read in conjunction with the Surrey MAISP. Organisations that are signatories to the C&D ISP are bound by the principles of the MAISP and are automatically a signatory to that overarching protocol.

The C&D ISP does not give agencies the automatic right to receive information or a mandate to provide information. It simply provides a safe framework within which signatory agencies agree to operate when sharing personal or sensitive information.

See **Appendix One** for definitions of the terms personal, sensitive and de-personalised or non-personal information.

4. Purpose

The purpose of the C&D ISP is to:

- Provide a framework for the exchange of personal or sensitive information to assist multi-agency partners in reducing crime, disorder and anti social behaviour, protecting vulnerable victims, and the implementation of Community Safety Partnership Plans
- Ensure all partners involved in multi agency problem solving meetings such as Community Incident Action Groups (CIAGs), Joint Action Groups (JAGs) and Multi Agency Risk Assessment Conferences (MARACs) understand their responsibilities with regard to information sharing
- Facilitate the sharing of relevant personal or sensitive information between partner organisations with respect and confidentiality, while safeguarding the legal rights of individuals
- Promote trust between partner organisations and the public

Sharing information is fundamental to the success of any strategy to reduce crime, disorder and anti social behaviour. It is vital that agencies working with those at risk of offending and their victims, or involved in securing legal orders such as Injunctions or Closure Orders, share information within a safe and legal framework.

5. Impact

Information sharing relies on good relations between partners, and above all mutual trust. The effectiveness of information exchange arrangements is a reflection of the effectiveness of the partnership as a whole.

The impact of effective information sharing is:

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

6. Organisations covered by this protocol

This protocol covers the information sharing activities of the responsible authorities that make up the 11 district and borough based Community Safety Partnerships (CSPs) in Surrey, as defined by Sections 5-7 of the Crime & Disorder Act 1998. These are:

- Police
- Local Authorities (district/borough council, unitary and/or county council)
- Fire & Rescue Authorities
- Probation
- Health

These responsible authorities work together to protect their local communities from crime and to help people feel safer. They work out how to deal with local issues like antisocial behaviour, drug or alcohol misuse and reoffending. They annually assess local crime priorities and consult partners and the local community about how to deal with them.

This protocol also covers those organisations that CSPs are expected to work in cooperation with, and whose knowledge could assist the CSP to reduce crime and anti social behaviour more effectively, such as:

- Parish Councils
- Registered Social Landlords
- Drug and Alcohol Services
- Town Centre Management
- Schools
- Victim Support
- Restorative and Rehabilitation Services
- Voluntary organisations

7. The legal framework for Crime & Disorder Information Sharing

All parties in this Protocol undertake to co-operate fully with each-other, within the parameters of the following acts:

- Crime and Disorder Act 1998
- Data Protection Act 1998
- Human Rights Act 1998
- Common Law Duty of Confidentiality

Crime and Disorder Act 1998

Section 115 of the Crime and Disorder Act allows for the exchange of information to a responsible authority where that disclosure is necessary or expedient to support delivery of the local strategy to reduce crime and disorder, the youth justice plan, or any other purpose of the Act.

Data Protection Act 1998

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 Act does require a structured approach to the handling of personal information and clear procedures for processing this information.

See **Appendix Two** for the eight principles of Data Protection.

Human Rights Act 1998
The Human Rights Act 1998 gave effect in UK law to the rights contained in the European Convention on Human Rights (ECHR). Article 8 states that everyone has the right to respect for his or her private and family life, their home and their correspondence. However, this right is not absolute and information sharing can be justified in the interests of the prevention of crime and disorder.

Common Law Duty of Confidentiality
The duty of confidentiality has been defined by a series of legal judgements and is a common law concept rather that a statutory requirement. Personal data which is seen as subject to this duty includes information that is not already in the public domain, has a certain degree of sensitivity, or was provided on the expectation that it would only be used or disclosed for particular purposes. However, the common law judgements have identified a number of exceptions, which includes the need to prevent, detect and prosecute serious crime. (Serious crime involves the use of violence; results in substantial financial gain; or is conducted by a large number of persons in pursuit of a common purpose).

The revised Caldicott principles
Caldicott principles govern information sharing in health settings. In 1997, the Caldicott committee presented its report on patient confidentiality. The impetus behind this was concerns about patient information and security. In September 2013 the Department of Health published a review of Caldicott and a revised set of principles which now include: "The duty to share information can be as important as the duty to protect patient confidentiality".

There are many legislative frameworks that control the exchange of information in the fulfilment of public sector responsibilities. These can be found in Appendix 1 of the Surrey MAISP.

REMEMBER that the Data Protection Act 1998, Human Rights Act (1998) and the Common Law Duty of Confidentiality are not barriers to sharing information but provide a framework to ensure that personal information about living persons are shared appropriately.

8. The Agreement

By signing up to this protocol, signatories are committed to cooperation with partners and will apply a positive approach to information sharing for the purpose of preventing or detecting crime, disorder and anti social behaviour and protecting vulnerable victims.

Signatories agree to meet the commitments outlined in this C&D ISP and abide by the principles and processes outlined in the overarching Surrey Multi-Agency Information Sharing Protocol (MAISP) in all instances of information sharing.

It is the responsibility of each signatory to ensure that:

Their organisation abides by the Golden Rules for information sharing in all instances of information exchange, provided in **Appendix Three**

- The information is shared, received and stored securely
- Information sharing is in accordance with the law
- Information is shared responsibly and in accordance with professional and ethical standards
- Realistic expectations are established from the outset regarding the reasons for which the information is required and the purposes for which it will be used
- Professional ethical standards are maintained
- Information exchanges and refusals are recorded in such a way as to provide an auditable record

- Providers of information are consulted 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 provider of the information as soon as is practicable.
- Any electronic information exchange is fully secure
- Arrangements are in place, to test that this agreement, its associated working practices and legal requirements are being adhered to
- The information shared will only be used for the purpose for which it was requested, and it will be securely exchanged, stored and destroyed when no longer required.

The Surrey MAISP provides forms and procedures which, when followed, will ensure signatories to this protocol meet the responsibilities listed above.

Training

All organisations covered by this protocol will ensure individuals involved in information sharing under this protocol are trained to a level that enables them to undertake their duties confidently, efficiently and lawfully. This is an obligation on each partner organisation and responsibility for it cannot be assigned to another organisation, although delivery of training can with that third party's consent.

To minimise the costs associated with training, and to ensure a consistent approach to information sharing, it is strongly advised that partners collaborate in the development and delivery of training.

In Surrey the use of the secure web-based case management system SafetyNet is strongly advised to ensure timely and secure electronic information sharing. You can email: Joanna.grimshaw@surrey.pnn.police.uk to arrange SafetyNet training and access for your organisation.

9. Signatories and Designated Officers

Signatories to this protocol may choose to assign specific staff to facilitate, manage or advise on information sharing. These may be existing data protection, information security or information governance staff. It is anticipated that most organisations will nominate the following roles:

Information Sharing Leads will:

- Contribute to reviews of the C&D ISP or related processes as required
- Ensure that the C&D ISP requirements are reflected in training, data security or management and complaints processes

Designated Officers

Signatories may choose for all or most information sharing to be channelled through Designated Officers or they may decide that it is more practicable for Designated Officers to take a consultative role, advising staff on information sharing when required.

Designated Officers may be assigned the following responsibilities:

- To be fully aware of the principles and processes of the C&D ISP and those of the Surrey MAISP
- To contact DOs in other signatory organisations to request information sharing and to be a point of contact for DOs in other signatory organisations
- To participate in multi agency meetings where personal and confidential information is exchanged under the C&D ISP where required

- To ensure that the 'Golden Rules' are complied with when they share information
- To maintain appropriate records of all information sharing matters that they have been involved in, including notes from relevant meetings / correspondence
- To seek advice from their organisation's Information Sharing Lead or Data Protection Lead where necessary

Where practicable a person asking for information from another agency must make the request through a Designated Officer.

The Surrey County Council Community Safety Team will maintain a list of contact details for all Signatories and Designated Officers signed up to the C&D ISP.

Appendix One

Definitions of Types of Data

Personal Data

Personal data relates to specific information about a living individual who can be identified or, information which could be used by a data controller (or any person) to identify an individual. Typically, personal data would include information such as name, date of birth, address etc., but could also include other information that would be likely to identify an individual e.g. ethnicity if the individual was one of a few ethic minority residents in an area, or gender or age where this would allow the individual to be identified.

Sensitive Data

Sensitive data can include any of the following:

- Racial or ethnic origin
- The subjects political opinions
- Religious beliefs
- Sexual orientation
- Physical or mental health
- Trade union membership
- Any proceedings for offences committed and subsequent disposals

Depersonalised or Non-personal Information

This category encompasses any information which does not or cannot be used to establish the identity of a living individual as any reference to or means of identifying any living individual(s) has been removed. There are generally no legal restrictions on the exchange of non-personalised data.

Consideration should however be given to the fact that any disclosure made should be in accordance with internal organisational policy relating to the disclosure of information to other agencies (e.g. there may be certain sensitivities in relation to the information that, whilst not constituting personal day, may make disclosure harmful or inappropriate).

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

- No attempt must be made to identify an individual through the provision of depersonalised information
- Data sets must not be released to those who have a commercial interest in their use
- Arrangements must be made for the secure storage of all depersonalised information
- Information must be destroyed or returned to the data controller when it is no longer required

Non personalised information held by public sector agencies may be subject to the provisions of the Freedom of Information Act 2000 and disclosure may be required, if a lawful request is made to a public authority and there is a legal duty to provide it (certain categories of exemption may apply).

Appendix Two

Eight Principles of Data Protection

Data Protection Act 1998

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Schedule 2 sets out purposes for legitimate processing of information:

- Processing information with the permission of the data subject (the person who the information is about).
- If the processing is necessary for:
    - The performance of or entering into a contract with the data subject;
    - Enforcing the law, carrying out statutory functions and any functions of the Crown, a Minister of the Crown, or a government department, or carrying out any other function that is in the public interest.
    - Meeting any legal obligation that applies to the data controller
    - Protecting the vital interest of the data subject; and
    - The purposes of the legitimate interests of the data controller or anyone else who receives the information, as long as this will not affect the rights and freedoms or legitimate interests of the data subject

When processing sensitive personal information, a condition of Schedule 2 and a condition of **Schedule 3** must be met. The Schedule 3 conditions are:

- Processing with the permission (consent) of the data subject
- Processing that is needed to exercise a legal right or obligation in connection with employment
- Processing that is needed to protect the vital interests of the data subject, or anyone else if they do not give their permission
- Processing political, philosophical, religious or trade union information in connection with its legitimate interests by any non-profit making organisation
- Processing information made public as a result of something the data subject has deliberately done
- Processing that is needed in connection with legal proceedings, getting legal advice or exercising or defending legal rights
- Processing that is needed to enforce the law for and carry out statutory functions, exercise the function of the Crown, Ministers or government departments
- Processing medical information by medical professionals or others that have an obligation to keep the data subjects information confidential
- Ethnic monitoring

Appendix Three

Golden Rules of Information Sharing

Confirm the identity of the person you are sharing with

Obtain consent to share if safe, appropriate and feasible

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

Don’t share more information than is necessary

Inform the recipient if any of the information is potentially 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.

Appendix Four

Myth-Busting Guide

Sharing of information between practitioners and organisations is essential for effective identifications, assessment, risk management and service provision. Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children and young people, or other vulnerable individuals, at risk of abuse or neglect. Below are common myths that can act as a barrier to sharing information effectively:

The Data Protection Act 1998 is a barrier to sharing information

No – the Data Protection Act 1998 does not prohibit the collection and sharing of personal information. It does, however, provide a framework to ensure that personal information about a living individual is shared appropriately. In particular, the Act balances the rights of the information subject (the individual whom the information in about) and the need to share information about them. Never assume sharing is prohibited – it is essential to consider this balance in every case. The Information Commissioner has published a statutory code of practice on information sharing to help organisations adopt good practice.

Consent is always needed to share personal information

You do not necessarily need the consent of the information subject to share their personal information. Wherever possible, you should seek consent or be open and honest with the individual (and/or the family, where appropriate) from the outset s to why, what, how and with whom, their information will be shared. You should seek consent where an individual may not expect their information to be passed on and they have a genuine choice about this. Consent in relation to personal information does not need to be explicit – it can be implied where to do so would be reasonable, i.e. a referral to a provider or another service. More stringent rules apply to sensitive personal information, when, if consent is necessary then it should be explicit. But even without consent, or explicit consent, it is still possible to share personal information if it is necessary in order to carry out your role, or to protect the vital interests of the individual where, for example, consent cannot be given.

Also, if it is unsafe or inappropriate to do so, i.e. where there are concerns that a child is suffering, or is likely to suffer significant harm, you would not need to seek consent. A record of what has been shared should be kept.

Personal information collected by one organisation cannot be disclosed to another organisation

This is not the case, unless the information is to be used for a purpose incompatible with the purpose that is was originally collected for. In the case of a child at risk of significant harm, it is difficult to foresee circumstances where sharing personal information with other practitioners would be incompatible with the purpose for which was originally collected.

(Taken from the Department for Education document 'Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers, March 2015)

Appendix Five

Signatories to the Surrey Crime and Disorder Information Sharing Protocol

Up to date as at 24 October 2018

Please note: The Surrey Crime & Disorder Information Sharing Protocol (C&D ISP) is a context specific, tier two protocol that is compliant with the overarching Surrey Multi Agency Information Sharing Protocol (MAISP). Organisations that are signatories to the C&D ISP are bound by the principles of the MAISP and are automatically a signatory to that overarching protocol.

A2 Dominion
Abbeyfield North Downs Society
Ability Housing Association
Academy of Contemporary Music
Accent Housing Ltd
Alliance of Surrey Mediation Services
Ash Parish Council
Ashford & St Peter's Hospital NHS Foundation Trust
Avenues Trust Group
Bishop David Brown School
Browns Community Services CIC
Catalyst Support
Central Surrey Health
Clarion Housing Group
Crown Simmons Housing
Cuddington Croft Primary School
East Surrey College
East Surrey Domestic Abuse Services
East to West Trust
EIKON
Elmbridge Borough Council
English Rural Housing Association
Environment Agency
Epsom & Ewell Borough Council
Experience Guildford
Frimley Health NHS Foundation Trust
Fulham FC Foundation
Fullbrook School
Godalming College
Grange Management (Southern) Ltd
Greenoak Housing Association
Guildford Action
Guildford Borough Council
Guildford College of Further and Higher Education
Guildford Number Five Project
Guildford YMCA
Hanover Housing Association
Heathside School
Holmdene Housing
Home Group
Hyde Housing Group
Kingston Churches Housing Association

Leatherhead Start
London & Quadrant Housing Trust
Look Ahead Housing and Care
Magna Carta School
Mediation North Surrey
Metropolitan Housing Trust
Mid-Surrey Mediation Service
Moat Homes Ltd
Mole Valley District Council
Mount Green Housing Association
National Probation Service
National Trust
New Vision Homes
North Surrey DA Outreach (Citizens Advice Elmbridge (West)
Orbit South Housing
PA Housing
Radian
Raven Housing Trust
Reigate & Banstead Borough Council
Reigate School
Reigate Valley College
Richmond upon Thames Churches Housing Trust
Rosebery Housing Association Ltd
Runnymede and Spelthorne CAB
Runnymede Borough Council
Southern Housing Group
Spelthorne Borough Council
Stonewater Housing Ltd
Sunbury Manor School
Surrey and Borders Partnership NHS Trust
Surrey and Sussex Healthcare NHS Trust
Surrey County Council
Surrey Drug and Alcohol care limited
Surrey Heath Borough Council
Surrey Police
Tandridge District Council
Thames Valley Housing Association
The Amber Foundation
The Guinness Partnership Limited
The Riverside Group Limited
The Warwick School
Transform Housing & Support
University of Surrey
Victim Support Surrey
Voluntary Action Mid Surrey
Walton-on-Thames Charity
Warden housing association (home group)
Waverley Borough Council
West Surrey Mediation Service
Woking Borough Council
Women in Prison
YMCA East Surrey

York Road Project
yourSanctuary