Sharing Personal and Sensitive Personal Information on Children and Young People at Risk of Offending

A PRACTICAL GUIDE
CONTENTS

Introduction 2
Risk and protective factors 3
A lawful basis for sharing risk-factor information 6
Law of confidence 7
Data Protection Act 1998 7
Human Rights Act 1998 and Article 8, European Convention on Human Rights 10
Consent 11
Protocols 11
Conclusion 13
Practical application – a case study 14
Introduction

The purpose of this guidance is to support the development of multi-agency protocols that facilitate the exchange of personal data. Local authorities, police authorities, health authorities and others need to be able to share personal data in order to comply with their statutory duties to work together in support of children and young people at risk of future involvement in criminality. These duties include the development and implementation of strategies and tactics for preventing and reducing crime. By following this guidance, it should be clear that agencies are able to share personal data, even without the consent of the data subject, across a range of existing and planned partnership arrangements. These partnerships include:

- Youth Offending Teams (Yots)
- Safer School Partnerships
- Children’s Fund Partnerships
- Child Protection Teams
- Youth Inclusion and Support Programmes (YISPs)
- Information-sharing and assessment.

However, this document will be relevant to any partnerships that aim, principally or otherwise, to prevent crime by children and young people through the provision of early support and intervention to reduce identified risks.

Exchanging personal and sensitive personal information between agencies, without the consent of the data subject, is seen as difficult and this is often used as an excuse for not doing it. However, in the context of preventing or reducing crime and disorder, and given the legislative framework within which the agencies referred to in this guidance operate, such exchange of information can, in fact, normally be done lawfully. This guidance sets out how and why information-sharing in this context is lawful. It also includes a practical application tool in the form of a case study and a useful flow chart to illustrate how information-sharing can be straightforward and lawful, and result in effective intervention.

While agencies remain legally responsible for the data they hold, and any action they take with regard to it, it is hoped that this guidance will form a common basis for future multi-agency, electronic and other secure information exchange procedures.
concerning children and young people at risk. This guidance supports and enhances the development of a Common Assessment Framework by enabling multi-agency assessment to take place to identify cumulative risks and, consequently, the most appropriate early intervention and support to meet the needs of the child, young person, their parents/carers and wider family. These multi-agency partnerships will also need to establish their own data-sharing protocols for which useful generic advice is also provided.

This guidance only applies to personal and sensitive personal data – that is information about identifiable living individuals as defined in sections 1 and 2 of the Data Protection Act 1998. Information that does not relate in any way to a living individual can be shared freely in any event, and is not subject to the provisions of the Act. As well as the Data Protection Act 1998, this guidance takes account of the Human Rights Act 1998, Article 8 of the European Convention on Human Rights, and the common law of confidence.

Risk and protective factors

Extensive credible and predictive research into youth offending shows that there is a range of identifiable risk factors present in the lives of many children and young people. The presence of particular risk factors, or a combination of them, significantly increases the likelihood of children and young people becoming involved in criminal and anti-social behaviour. In addition, the research suggests that multi-agency identification of such risk factors provides the opportunity for earlier identification of those children and young people at greatest risk. The most effective prevention strategy would seek to identify collectively such high-risk children and young people. The sharing of risk-factor information in respect of them is vital in order to:

- identify those at greatest risk
- bring protective factors voluntarily into their lives
- prevent them becoming involved in crime and disorder.

In November 2001, the Youth Justice Board published the research report, Risk and Protective Factors Associated with Youth Crime and Effective Interventions to Prevent It.¹

¹ Communities that Care UK, Risk and Protective Factors Associated with Youth Crime and Effective Interventions to Prevent It, Youth Justice Board, 2001 – available at www.youth-justice-board.gov.uk/publications.
The research was conducted by Communities that Care and, drawing on a wealth of evidence from international research, it identifies the risk and protective factors associated with criminal or anti-social behaviour that can be found in the lives of children and young people. The report supports the early identification of these risk factors and makes it clear that the presence of multiple risk factors greatly increases the likelihood of a child or young person becoming involved in future criminal or anti-social behaviour.

The three significant risk factors highlighted by Communities that Care in the lives of their research sample were:

- low achievement at school, which was linked to truancy, exclusion, and poor attendance and attainment (increased the likelihood of criminal arrest by 90%)
- family problem behaviour, which was linked to family breakdown; criminal family member, abusive relationships and drug/alcohol use in the family (increased the likelihood of criminal arrest by 62%)
- peer involvement in behaviour, which was linked to criminal or anti-social peers, and truanting or excluded peers (increased the likelihood of criminal arrest by 50%).

However, the most significant factor, as identified in much research, relates to being male. The Communities that Care research identified an increased likelihood of criminal arrest by 146%, and Rutter et al (1998) listed being male among their three most significant risk factors, along with the onset of hyperactivity at an early age, and having a criminal family member.

Various researchers have separately identified a range of risk factors that increase the likelihood of subsequent offending when they are present in the lives of children and young people. The relevant risk factors typically identified by this research are:

- being male
- teenage pregnancy
- deprivation and unemployment
- criminal family member
- onset of hyperactivity at an early age
- broken/disrupted family lifestyle
- low attention span
- disruptive/anti-social behaviour
- mixing with offending peers
- poor/inconsistent parenting
- abusive parent
- truancy

Multi-agency identification of these risk factors is highlighted by the Communities that Care report as providing the best opportunity for the earliest identification of those children and young people at greatest risk of future criminality. Where four or more of these risk factors are present, the risk is sufficiently great to warrant structured consideration of voluntary support and intervention for the child or young person and their family from statutory agencies that are working together to reduce the risk.

Research further suggests that it is reasonable to group risk factors in four broad categories (these may be useful to some agencies and partnerships in directing resources). These are the impact of:

- the family
- the school
- personal and individual factors
- the community.

The sharing of information in respect of children and young people is vital in order to identify those at greatest risk, so they can be afforded services that will bring protective factors into their lives and prevent them becoming involved in crime and disorder. To achieve this, agencies involved in a partnership should agree a list of risk and protective factors appropriate to the partnership aims and objectives. A list of risk factors most applicable to the prevention of crime agenda has been compiled in the form of a table that allows space for justifying each individual risk identified in a young person’s life, and can be viewed at www.yjb.gov.uk/informationsharing (all other tools mentioned in this guidance can also be found at this address). In this format, it makes for a simple but effective multi-agency screening tool that will enhance any single agency use of the Common Assessment Framework currently being developed, and from which the overall level of perceived risk can be fully assessed.
Comprehensive information on any child or young person, or indeed on any specific risk factor in their life, is rarely held exclusively by a single agency. Consequently, some information held in different agency records about the same person will differ in emphasis, according to the nature of the agency holding it. ‘Risk-factor information by agency’ (available on the website, see p.5) provides a list of agencies likely to hold vital information on the relevant risk factors present in individual children and young people’s lives. It is not an exhaustive list of agencies, nor of the relevant information they may hold; but it is a useful indicator of how different and unrelated issues become relevant in this preventive context.

**A lawful basis for sharing risk-factor information**

In order to be able to share personal information at all, a public body must have some lawful basis for doing so. This may stem from common law or prerogative powers (for non-statutory bodies such as the police), or be implied or expressly conferred by statute.

Agencies are increasingly required by government and under statute to work together in tackling different negative aspects of the lives of children and young people, and to support their positive development into adulthood. The stated bodies holding the information which may be required in order to identify and tackle the risk potentially posed to, and by, children and young people, and for whom this guidance has been developed, are:

- local authorities*
- chief officers of police**
- police authorities**
- strategic health authorities***
- health authorities***
- local probation boards
- local education authorities
- Primary Care Trusts***
- local housing authorities.

* ‘Local authorities’ covers all services for which they are responsible, including social services, education services, children’s services, housing services, etc.

** ‘Chief officers of police’ and ‘police authorities’ covers all police services for which they are responsible.

*** ‘Strategic health authorities’, ‘health authorities’ and ‘Primary Care Trusts’ between them cover all health services for which each has responsibility, including child and adolescent mental health services (CAMHSs), etc.
Although a Youth Offending Team (Yot) is not in itself a legal entity, it is a statutory partnership of named local agencies, which are all listed above: as such, this guidance applies equally to data-sharing within and by a Yot.

Through a variety of common law, prerogative powers, and legislative provisions, all of these bodies have the required lawful basis for disclosing personal information for the purpose of preventing or detecting offending by children and young people. The statutory provisions considered relevant to each of the bodies listed above are set out in detail in ‘Background legislation’ (available on the website, see p.5).

**Law of confidence**

Even where there is a prima facie lawful basis for information-sharing, it may be that some of the information held by the relevant bodies is such as to come under the common law duty of confidence. Where this is the case, the body cannot disclose such information without the consent of the individual concerned, unless there is either a legal obligation to do so, or an overriding public interest in favour of disclosure. In the context of the information-sharing considered by this guidance, disclosures will sometimes be pursuant to statutory duties (see ‘Background legislation’ on the website). Where there is no statutory duty to disclose, because of the context and purpose of the proposed information-sharing it is considered that an overriding public interest in disclosure is likely to arise such that disclosure can still be made. It is therefore considered that the law of confidence should rarely prevent disclosures in the current context.

**Data Protection Act 1998**

Once a lawful basis for the sharing of information is established, any actual disclosure must comply with the Data Protection Act. The Data Protection Act regulates the processing of personal and sensitive personal data (as defined in sections 1 and 2 of the Data Protection Act). Processing of personal data must comply with the requirements of all eight data protection principles specified within the Data Protection Act unless, and to the extent that, an exemption applies. For processing, which consists of ‘disclosing’ personal data within the UK, the most relevant data protection principles are the first five.

- **First data protection principle**
  
  ‘Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
i) at least one of the conditions in schedule 2 is met

ii) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.’

■ Second data protection principle

‘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.’

■ Third data protection principle

‘Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.’

■ Fourth data protection principle

‘Personal data shall be accurate and, where necessary, kept up to date.’

■ Fifth data protection principle

‘Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.’

A checklist for ensuring that a legal basis exists for the sharing of personal and sensitive personal information in compliance with schedules 2 and 3 of the Data Protection Act appears opposite in the form of a flow chart.
CHECKLIST FOR INFORMATION-SHARING IN ACCORDANCE WITH DATA PROTECTION ACT SCHEDULES 2 AND 3 CONDITIONS OF THE FIRST DATA PROTECTION PRINCIPLE

START HERE

Are data personal? (this includes sensitive personal data)

Yes No

(Sch. 3. para 1) Has data subject given explicit informed consent to this sharing of personal data?

Yes No

(Sch.2. para.5(a) and sch.3. para.7(i)(a)) Is data-sharing necessary for the administration of justice?

Yes No

(Sch.2. para.3(b&c) and sch.3. para.7(iii)(a)) Is data-sharing necessary for the exercise of functions (a) conferred by or under any enactment or (b) of the Crown, minister of the Crown or a government department?

Yes No

Are any data sensitive personal data?

No Yes

(Sch.2. para.4) Has data subject given any consent to this sharing of personal data?

Yes No

DATA PROTECTION ACT 1998 DOES NOT APPLY

Do not share data there is no legal basis within the data protection act 1998 for doing so

No Yes

(Sch.3. para.10) Is data-sharing permitted under any other provision of the Order made under paragraph 10 of schedule 3 (see ‘Background legislation’, available on the website) e.g. is it necessary for exercise of any functions conferred on a constable by any rule of law?

No Yes

(Sch.3. para.6(a)) Is data-sharing necessary to pursue legitimate interests of data controller or receiver, without unwarranted prejudice to the data subject?

No Yes

(Sch.3. para.8(i)(a)) Is data-sharing necessary for medical purposes and undertaken by health professional?

Yes No

(Sch.3. para.6(a)) Is data-sharing necessary for purpose of connection with any legal proceedings, now or in future?

No Yes

Are any data sensitive personal data?

Yes No

(Sch.3. para.3) Is data-sharing necessary to comply with any legal obligation?

No Yes

DATA-SHARING COMPLIES WITH REQUIREMENTS OF SCHEDULES 2 AND 3 OF THE DATA PROTECTION ACT 1998
In respect of information-sharing for the purpose of preventing or detecting crime by children and young people, each body making a disclosure in accordance with an appropriate data-sharing protocol can very probably do so fully in compliance with the Data Protection Act, either because the disclosure meets all of the requirements of these data protection principles, or as a result of applying an exemption from certain elements of the principles. An important question when considering whether the data-protection principles have been met in any particular case is likely to be the necessity and proportionality of the disclosure. Proportionate disclosure is disclosure necessary for one of the purposes set out in the Data Protection Act, and which is no wider or greater than is needed to achieve that purpose.

In applying the Data Protection Act exemptions, the most relevant exemption in this context is section 29, which relates in certain circumstances to the prevention or detection of crime. It is also possible that, in some cases, the exemption provided for in section 35(1) might be applicable. This provides an exemption from some of the requirements of the Data Protection Act, where a disclosure is required by or under any enactment. Further guidance on compliance with all eight principles, plus the operation of sections 29 and 35(1) exemptions can be found in ‘Background legislation’ (available on the website, see p.5).

**Human Rights Act 1998 and Article 8, European Convention on Human Rights**

Another provision relevant to information-sharing is Article 8 of the European Convention on Human Rights, which confers on everyone ‘the right to respect for his private and family life, his home and correspondence’. The disclosure of personal data by one body to another may well amount to an interference within the meaning of Article 8(1), but interferences are permitted in the circumstances set out in Article 8(2). For instance, a lawful interference can be made, where necessary, for the prevention of disorder or crime, or to protect the rights and freedoms of others, provided the interference has some foreseeable lawful basis and is a proportionate measure, given the aim it is seeking to achieve. These criteria will generally be met for data-sharing carried out in the context to which this guidance applies. Consequently, any such data-sharing is likely to be compatible with Article 8. The best way to ensure compatibility is, generally, to carry out data-sharing in accordance with an appropriate data-sharing protocol.
**Consent**

Consent, although desirable, is not essential for agencies to share personal information in the circumstances envisaged in this guidance. In relation to the first data protection principle, which requires fair processing, consent is simply one of a number of conditions set out in schedules 2 and 3 to the Data Protection Act (see flow chart, p. 9). Accordingly, providing one of those other conditions is met, consent is not necessary.

However, obtaining consent remains a matter of good practice, as opposed to a requirement of law, where the purpose of sharing information is not prejudiced by notifying the data subject at that time. An example form for recording consent, ‘Individual consent to personal information disclosure’, can be found on the website (see p. 5). In practice, because of the voluntary nature of preventive support and intervention, the direct involvement of the data subject will be necessary at some stage. Any need to share personal information without consent is, therefore, expected to be minimal and is likely to be restricted to the early identification stage of those children and young people who are at risk. Further details on the issue of consent can be found in the ‘Consent’ section on the website (see p. 5).

**Protocols**

Data-sharing should normally be carried out in accordance with an appropriately framed data-sharing protocol in order to ensure compliance with the various legal rules governing data-sharing as outlined previously. This is advisable because data-sharing must be proportionate to the legitimate objective pursued, and those requested to share personal information need to be confident that the highest standards, agreed in advance, will apply, and that the information will only be used for agreed and legitimate purposes. Agencies will need to ensure that:

- data is only shared where necessary
- the data shared and the circle of bodies to which it is communicated is no wider than is required for the legitimate objective pursued
- appropriate safeguards against errors and abuse are in place.

Since prevention is a relatively new issue for many partnerships, agencies working in this field will need to put in place mechanisms for the sharing of relevant information. This will involve making an assessment of the sources of information available and designing information flows that will facilitate the work of the partnership. This should
all then be framed within a jointly agreed information-sharing protocol designed to facilitate the stated purpose of the partnership. Each protocol must be specific to the stated purpose and signed by a senior representative from each partner agency. An example of a comprehensive protocol that can be simply modified for this purpose can be found online at www.crimereduction.co.uk/infosharing21.

Agencies and other partners will need to show that they are committed to the concept of working together to prevent and reduce crime committed by children and young people, and to doing so in an ethical manner and in the context of the duties conferred upon them under the:

- Crime and Disorder Act 1998
- Children Act 1989
- Learning and Skills Act 2000

It will be the responsibility of each agency, in accordance with this guidance, to ensure the following.

- Data-protection principles are adhered to unless an exemption applies.
- Realistic expectations prevail from the outset.
- Ethical standards are maintained.
- A mechanism exists by which the flow of information can be controlled.
- Appropriate training is provided.
- Adequate auditing arrangements exist to test adherence to the protocol.

Staff from each agency or organisation named in the protocol, who are working with children and young people in the partnership, should administer the protocol on a day-to-day basis, with discreet monitoring of compliance by their own data protection officer. Examples of standard forms of authority for sharing personal information by specific request on an inter-agency basis, or routinely within multi-agency partnerships, can be found on the website (see p.5).

Where an information-sharing protocol exists in respect of a multi-agency partnership, the purpose of which is to prevent crime and anti-social behaviour by children and young people, it is advisable for the practitioners in each agency to authorise the
shar|ing of information in accordance with that protocol on each occasion. Any suggestions for deviation or change in the terms of the protocol for individual cases must be presented, in the first instance, to the data controller of the agency that possesses the information. The data controllers from all partner agencies must agree any permanent change to the protocol.

More detailed information on data-sharing protocols can be found on the website (see p.5).

**Conclusion**

This guidance can most usefully be summarised as follows.

- Research proves the link between identified risk factors present in the lives of some children and young people, and their future involvement in crime and anti-social behaviour.

- Individual agencies working in isolation are unlikely to be aware of all the information they need to work effectively with young people at risk.

- Agencies are increasingly being required by government to work together to tackle those risk factors and thereby prevent crime and social exclusion generally; and a duty to work together to prevent crime and anti-social behaviour by children and young people is placed upon a variety of agencies by the Crime and Disorder Act 1998, the Learning and Skills Act 2000, the Criminal Justice and Court Services Act 2000, the Children Act 1989 and the Children Act 2004.

- The exercise of statutory functions conferred upon agencies by various enactments is specified in the Data Protection Act as an alternative ground for consent to sharing personal information where necessary.

- The prevention of crime and disclosures required by law are specifically included in the Data Protection Act as statutory exemptions from the need to comply with some, but not all, data protection principles and other requirements of the Data Protection Act.

- The consent of the data subject to the sharing of personal information is not normally required in this particular context. However, it is good practice to obtain consent where and as soon as possible.
The common law duty of confidence should rarely prevent disclosures in the context of preventing crime by children and young people.

The original purpose for which the personal information was obtained does not restrict the reuse of that information for other purposes in cases where the crime exemption in the Data Protection Act applies and where the objective of preventing crime would be prejudiced by not sharing it.

The statutory agencies for which this guidance has been developed should, by the implementation of appropriate procedures, be able lawfully to share relevant personal information in a partnership approach, to prevent the risk of involvement in criminality for children and young people.

Practical application – a case study

In practice, there are likely to be two significant episodes of personal data-sharing in the context of crime prevention. The first will be to identify those at sufficiently high risk of being involved in future criminality. The second will be to determine all the risks experienced by identified young people in order to design the most appropriate preventive support and intervention. In the first instance, it is unlikely that the data subjects will be aware of the data-sharing. However, in the second instance, it is good practice to involve the data subjects and their parents/carers in the planning of appropriate support and intervention in order to achieve their acceptance of it, given the fact that their participation will be purely voluntary. In either instance, it has already been made clear that, in appropriate circumstances, agencies can share personal data with or without the consent of the data subject. Wherever personal data is shared between agencies, each agency should keep a record of:

- the date
- the information shared
- with whom it was shared
- the purpose.

The case study below is not untypical of many young men who end up committing serious criminal offences. A step-by-step approach has been used to demonstrate that the sharing of risk-factor information on a multi-agency basis is valid, lawful and beneficial to the young person. The case study of “A” is also not unique in the range of contacts he has had with different statutory agencies during his life. Examination of
this case study reveals the existence of numerous recognised risk factors, and further analysis of the agencies that would be recording this information today highlights the need for multi-agency data-sharing to prevent crime. The step-by-step approach could start anywhere in this case study, but begins with “A” at the age of eight.

**Case study**

“A” is male, aged twenty-two, charged with an offence of robbery and remanded in custody awaiting trial.

His mother was 15 years old when he was born and living on a run-down council estate with his unemployed father who was aged 19 years and already a persistent offender with convictions for offences of violence and dishonesty. The family was given advice and support by social services until the mother was 16 years old, when she declined any further assistance, following her marriage to the father. At age two, the health visitor noted that “A” was hyperactive and causing anxiety in his mother who was eight months pregnant with a second child. This child, “A”’s sister, was subsequently born while their father was serving a prison sentence for burglary.

On commencing infant school, the teacher recorded that “A” was a bright boy, but had a very short attention span and a tendency to be disruptive in class. At junior school, this pattern continued and the first incident of bullying was recorded against him. It was also noted that he always appeared to be at the centre of any disruption to school life. When he was eight years old, the police had occasion to take “A” home after he was found at 1.00 a.m. walking the streets with a group of teenage boys. During his first year at secondary school, “A”’s father was convicted of raping “A”’s sister, and sentenced to eight years imprisonment. Since their father was remanded in custody from the outset, no continuing child protection concerns were identified in respect of “A” or his sister. The discovery of the theft of £5 by “A” from his mother’s purse was recorded by the social worker as a consequence of the current disruption to his life and not reported to the police.

The behaviour of his fellow pupils towards him became more abusive and insulting about his father, and “A” reacted by becoming more violent towards
them. This behaviour was condoned by his mother as a way of protecting “A” and his sister. At age 12, “A” was suspended from school for two weeks for violent behaviour and truancy. During this time “A” had received two police cautions for separate incidents of violence and had been reported to the police as missing overnight by his mother. At age 13, “A” was permanently excluded from school following an incident where he threatened a member of staff with a craft knife. By that time there were three further missing reports from his mother and he had been convicted of shoplifting and further cautioned for possession of cannabis.

At age 14, “A” was taken into local authority care when his mother could no longer cope with his behaviour. By age 16, “A” was sentenced to two years in custody for burglary, had been subject to numerous children’s home and foster placements, reported missing on eight occasions by social services – once for over a week – and convicted on three occasions for violence and dishonesty. Since his first release at age 17, his probation officers report that “A” has drifted between periods of detention from one area to another looking for a new start, but always turning back to crime.

**Step 1 – Initial referral**

The police have concerns about an eight-year-old boy, “A”, who was found roaming the streets at 1.00 a.m. with a group of older boys aged 15 to 17 years. The group was stopped in order to be questioned about complaints of disruptive behaviour. It was clear to the police officers that many had been consuming alcohol. When taken home, “A”’s mother appeared unconcerned and said that “A” often stayed out late with his mates. The mother was quite aggressive towards the police, insisting that “A” was in the protection of his older cousin.

The police decide that there is a need for a multi-agency risk assessment to be carried out on “A”, without the consent of the parents, who it is believed may be obstructive. They make a referral to the local partnership, giving the information shown overleaf.
Depending on local resources, this referral might be shared electronically or manually, and local arrangements would determine whether the process involved a regular face-to-face partnership meeting, a partnership meeting called on a needs-led basis, or a purely postal exercise at this initial information-sharing stage. The need for a partnership meeting, in the latter case, could be determined by an initial assessment of the information made available from each agency.

**Step 2 – Data-sharing**

Each agency involved in the partnership determines what, if any, of the information they hold is relevant to the purpose, and justifies the sharing of each item of personal and sensitive information with one or more other agencies (as appropriate) without the consent of the data subject.

In this case, it could be argued that there are two purposes to be served by multi-agency information-sharing: child protection and the prevention of crime. The police have already identified evidence of “A” being exposed to a risk of significant harm and the existence of recognised pre-crime risk factors in his life. The purpose of sharing information at this stage is to assess the extent of risk to “A” and, if necessary, to determine what action is required to protect him from harm and prevent his involvement in criminality.
The police

Identification details of subject
Name, date of birth, home address of “A”
School attended (if applicable)
Criminal record (if applicable)
Name of parent(s)/guardian(s)

Circumstances/concerns giving rise to referral
The subject was found at 1.00 a.m. (day, date) in (location) with a group of six other youths aged 15 to 17 years. These youths are known to be disruptive on the estate, and three of them have convictions for theft, taking a vehicle without consent and assault. One of the 16-year-olds is a cousin of “A”. “A” was considered to be vulnerable, and he was taken home by the police. His mother was aggressive to the police officers, saying “A” often goes out with his mates, his cousin was looking after him, and that it was nothing to do with the police.

Risk-factor information to be shared with other groups
- Criminal family member – the criminal convictions of “A’’s father and continuing suspicion of his involvement in crime
- Mixing with offending peers – the circumstances of finding “A” and the details and criminal convictions of the youths he was with, including evidence that many of them are known to be disruptive on the estate
Justification for sharing information

- Prevention of crime – to reduce the risk of “A” offending now or in the future – Crime and Disorder Act 1998, sections 6, 17, 37 and 38. Being male, with a criminal family member, and mixing with offending peers are all recognised risk factors for future involvement in criminality.

- Child protection – to protect “A” from harm – the local authority will also be able to facilitate data-sharing with the police, among others, in reliance on Children Act 1989, sections 17 and schedule 2, part 1. The circumstances of “A” being found at 1.00 am, and the attitude of his mother towards it, expose “A” to a greater risk of significant harm.

Legal and data protection issues

First principle – Data-sharing between relevant agencies in these circumstances will be lawful pursuant to the police’s common law powers, as well as pursuant, for example, to powers under section 27 Children Act 1989 and section 115 of the Crime and Disorder Act 1998. Relevant agencies do not need to provide fair processing information to “A” and his parents, either because they are obliged or authorised by statute to provide it, or because the section 29 crime exemption will apply. The conditions of schedules 2 and 3 of the Data Protection Act are also satisfied through the exercise of the functions conferred by the Children Act and Crime and Disorder Act respectively (see ‘Background legislation’ on the website, see p. 5).

Second principle – The partnership should have given notification to the Information Commissioner of its general purpose in sharing personal and sensitive personal data, i.e. child protection or prevention of crime. Unless the requirement to share data is directly contradictory with the purpose for which it was obtained, this information-sharing complies with the second data protection principle. In any event, where the crime prevention purpose is prejudiced by not sharing data, the section 29 exemption can be applied.
Third principle — Each agency should share the minimum amount of relevant information to fulfil the stated purpose of protecting “A” from harm and criminality.

Fourth principle — Each agency should take reasonable steps to ensure data are accurate and kept up to date. Wherever possible, the date of original entries and any updates should always be shown in data records, and efforts should be made to keep data updated to avoid damage or distress to “A”. While an exemption may be applied to this principle, best practice would be to maintain data accuracy wherever possible, i.e. in compliance with existing local agency data-protection policies and processes.

Fifth principle — Each agency should review their data regularly and delete that which is no longer required for the purpose. It is suggested that this should be done every six months for data shared for the purpose of preventing crime, and every 12 months for the purpose of child protection. The prevention of crime exemption can be applied, but best practice would be to weed out data that are no longer required because the purpose has been served. It is suggested that the data should be kept until the first six-monthly data review following completion of any agreed action plan by “A”.

Sixth principle — Each agency must respond to a subject access request and comply with any notices given under sections 10, 11, 12 and 12A of the Data Protection Act unless providing this information to “A” will prejudice the purpose. In this case, the exemption may be applied and some or all personal data can be withheld from “A”.

Seventh principle — Each agency should ensure the security of all personal data against unauthorised or unlawful processing or accidental loss, damage or destruction.

Eighth principle — Each agency should ensure that personal information is not shared outside member states of the European Economic Area.
Health services

Identification details of subject
Name, date of birth, home address of “A”
Name of parent(s)/guardian(s)
School attended

Circumstances/concerns giving rise to referral
See ‘Police’ referral (page 18).

Risk-factor information to be shared with other groups
- Teenage pregnancy – details of the birth of “A” to a young teenage mother
- Onset of hyperactivity at early age – details of “A”’s hyperactivity at two years of age

Justification for sharing information
- Prevention of crime – to reduce the risk of “A” offending now or in the future – Crime and Disorder Act 1998, sections 17, 37 and 38
- Child protection – to protect “A” from harm – the local authority will also be able to facilitate data-sharing with the strategic health authority (among others) in reliance on Children Act 1989, sections 17 and 27 and schedule 2, part 1
Legal and data protection issues

See information from ‘Police’ referral (page 18).

Client/patient confidentiality presents additional considerations for health services staff. It can be argued, on a case-by-case basis, that the public interest, including that of “A”, in preventing crime and protecting “A” from harm outweighs the need to maintain confidentiality about the relevant risk-factor information identified. Particular care should be taken to ensure that confidential medical information is only disclosed when necessary, and only to the extent necessary.

Local authorities (including, in particular, social services)

Identification details of subject

Name, date of birth, home address of “A”
Name of parent(s)/guardian(s)
School attended

Circumstances/concerns giving rise to referral

See ‘Police’ referral (page 18).

Risk-factor information to be shared with other groups

- Teenage pregnancy – details of the birth of “A” to a young teenage mother
- Poor parenting – details of the need for, and outcomes of, parenting advice and support given to the mother of “A” following his birth, including her generally unco-operative nature
**Justification for sharing information**

- Child protection – to protect “A” from harm – Children Act 1989, sections 17 and 27 and schedule 2, part 1
- Prevention of crime – to reduce the risk of “A” offending now or in the future – Crime and Disorder Act 1998, sections 17,37 and 38

**Legal and data protection issues**

See information from the ‘Police’ referral (page 18).

**Schools/education**

**Identification details of subject**

Name, date of birth, home address of “A”
Name of parent(s)/guardian(s)
School attended

**Circumstances/concerns giving rise to referral**

See ‘Police’ referral (page 18).
Risk-factor information to be shared with other groups

- Low attention span – the infant school report concerning “A”’s disruptive behaviour in class in relation to his low attention span
- Bullying – the junior school report of incidents when “A” was involved in bullying and in general unacceptable behaviour

Justification for sharing information

- Prevention of crime – to reduce the risk of “A” offending now or in the future – Crime and Disorder Act 1998, sections 17, 37 and 38
- Child protection – to protect “A” from harm – the local authority will also be able to facilitate data-sharing with the local education authority (among others) in reliance on Children Act 1989, sections 17 and 27 and schedule 2, part 1

Legal and data protection issues

See information from the ‘Police’ referral (page 18).
Step 3 – Data-handling

Once information has been shared with one or more other public bodies as appropriate, it can be compiled to show the full extent of the risk faced by “A”. An example of a useful screening form for this purpose is shown in ‘Background legislation’ on the website (see p. 5).

A number of options exist in relation to the data, following the assessment of risk to “A”. A lead agency should normally be appointed on a case-by-case basis to handle the combined data, with each of the other agencies retaining only the information they originated. Alternatively, where necessary and appropriate, each agency could retain the combined data that relate to their statutory responsibility and role in this continuing case. In either situation, “A” and his parents should be informed as soon as possible about the information-sharing; this could be done at the time when their voluntary co-operation with the action plan is sought. Where no action is required in terms of support, intervention or monitoring, the shared data should be destroyed by each agency apart from that originating from them. In every case, data should not be retained longer than is necessary for the stated purpose.

Wherever shared data are retained, they should be stored in accordance with the existing data protection policy within each agency. In order to ensure compliance with individual agency policies, joint data protection audits should be undertaken annually, and agreement reached to delete or retain specific personal data accordingly. This process would need to be incorporated within agreed data-sharing protocols for each partnership.

Step 4 – Action-planning

Irrespective of the local arrangements for the information-sharing step of the process, a partnership meeting will be required to determine the need for, and content of, any multi-agency voluntary action plan that provides support and intervention for “A”. Best practice involves the young person and their parents/carers at this stage. The plan should be designed to engage with “A” and his family, either through a single lead agency or, where necessary and appropriate, a multi-agency approach. This action plan should include further partnership meetings or case conferences, together with active interventions by the various agencies.
The content of the action plan should be determined with the full involvement of “A” and his parents. Within the action plan, it would be useful to include:

- the agreed aims and objectives
- who will be the lead agency
- the agreed responsibilities, including timescales, of each agency
- the agreed responsibilities of “A” and his parents/carers
- the capacity to incorporate information on progress and completion against each of the objectives.

The multi-agency voluntary action plan might look like that shown opposite.
MULTI-AGENCY VOLUNTARY ACTION PLAN IN RESPECT OF “A”

Lead agency: School

Aims:

a. To protect “A” from significant harm.
b. To protect “A” from involvement in anti-social behaviour and criminality

<table>
<thead>
<tr>
<th>Objective</th>
<th>Responsibility</th>
<th>Timescale</th>
<th>Progress</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide additional support for “A” in school.</td>
<td>School</td>
<td>Immediate 2 hrs per day to decrease with improvement.</td>
<td>Week 3 – 1 hr per day. Week 7 – 2 hrs per week.</td>
<td>Week 12 – behaviour good – ad hoc support at request of “A”.</td>
</tr>
<tr>
<td>“A” to be at home by 9.00 p.m. each night or with appropriate adult.</td>
<td>“A” + parents/carers – police to monitor at random.</td>
<td>Duration of multi-agency involvement.</td>
<td>Week 2 – in. Week 4 – at friends house. Week 7 – in. Week 10 – in.</td>
<td>Week 12 – in.</td>
</tr>
<tr>
<td>Parents/carers to attend voluntary parenting course.</td>
<td>Parents/carers, social services.</td>
<td>Duration of course.</td>
<td>Week 6 – full attendance.</td>
<td>Week 12 – full attendance, course enjoyed.</td>
</tr>
<tr>
<td>Provide psychological assessment if behaviour does not improve noticeably.</td>
<td>Education</td>
<td>After 6 months.</td>
<td>Week 4 – behaviour improving.</td>
<td>Week 12 – no longer required.</td>
</tr>
<tr>
<td>To monitor “A” and his family, and provide professional support as necessary at request of lead agency.</td>
<td>Police, health services, social services, education.</td>
<td>Duration of multi-agency involvement.</td>
<td>No contact reported or requested.</td>
<td>Up to week 12 – no contact of any concern to this plan.</td>
</tr>
</tbody>
</table>

We agree to support the objectives outlined above.

Signed: (all parties to the agreement)  
_________________________________________________________  Date: ____________________________

“A” is beginning to achieve to his potential at school and controlling his behaviour. His parents have successfully completed their parenting course. There are no outstanding concerns. We are satisfied that the objectives outlined above have been completed successfully, and that the aims should now be met without multi-agency involvement.

Signed: (all parties to the agreement)  
_________________________________________________________  Date: ____________________________
Step 5 – Partnership case closure

Progress of multi-agency voluntary action plans should be monitored for an appropriately defined period, to be determined on a case-by-case basis. After this period, all agencies should meet to decide whether to close the case. This will not necessarily mean the withdrawal of all support and intervention for “A”, but will end the need for multi-agency involvement. In “A”’s case, the agreement to close the case has been incorporated in the original action plan and was determined by the ‘Progress’ and ‘Completion’ entries in the table. Any data held by agencies that did not originate from them should then be deleted at the first six-monthly review of partnership data, following closure of the case.

While this outcome for “A” is hypothetical, his life chances could have been very much improved had he benefited from such multi-agency involvement. In order to apply the extensive lessons of predictive research to reduce the likelihood of young people becoming involved in crime, statutory agencies must work closely together and share relevant information if they are to meet their current statutory obligations. When four or more risk factors cluster together in the life of a child or young person, agencies, working together, should take steps to provide support and intervention to reduce those risks. The process may vary, but any agency should be able to instigate the multi-agency assessment of risk as soon as they have sufficient concern to do so. This guidance demonstrates how this can be done in full compliance with existing legislation.
Further copies of this document can be obtained from:
Telephone 0870 120 7400
Facsimile 0870 120 7401

Youth Justice Board for England and Wales
11 Carteret Street
London SW1H 9DL
Telephone 020 7271 3033
Facsimile 020 7271 3030
www.yjb.gov.uk