

Guidance on Disclosure and Sharing of Information

Antisocial Behaviour etc. (Scotland) Act 2004 Antisocial Behaviour etc. (Scotland) Act 2004



safer
scotland
SCOTTISH EXECUTIVE

© Crown copyright 2004

ISBN: 0-7559-4384-8

Scottish Executive
St Andrew's House
Edinburgh
EH1 3DG

Produced for the Scottish Executive by **Astron** B38020 10/04

Published by the Scottish Executive, October, 2004

Further copies are available from
Blackwell's Bookshop
53 South Bridge
Edinburgh
EH1 1YS

The text pages of this document are produced from 100% elemental chlorine-free, environmentally-preferred material and are 100% recyclable.

CONTENTS

Introduction	1
Contact	
Who is this Guidance For?	2
What Does the ASB Act Provide on Information Sharing?	3
How Does the ASB Act Relate to Data Protection and Other Law?	4
Data Protection Act 1998	
Misconceptions about Data Protection Law	
Human Rights Act 1998	
The Common Law Duty of Confidence	
Protocols	10
Requests to Disclose and Share Information	
Requests from the Police	
Requests to the Police	
Conclusion	14
Annex A – Model Protocol	15
Annex B – Glossary of terms in Model Protocol	27

INTRODUCTION

1. Tackling antisocial behaviour is increasingly a major part of the work of a wide range of agencies and groups - local authorities, police, social landlords, children's reporters, voluntary organisations, parts of the private sector and community bodies, including members of the public.

2. The Antisocial Behaviour etc. (Scotland) Act 2004 ("the 2004 Act") is intended to help deal with antisocial behaviour more effectively. It contains a range of provisions in the areas of justice, the environment, housing and child welfare, all of which are linked to tackling antisocial behaviour. The Act can be accessed at www.hmsso.gov.uk

3. One of the major obstacles to dealing effectively with antisocial behaviour has been difficulties around disclosure and sharing of information. There has been a lot of confusion about what practitioners can and cannot do when it comes to sharing information. In part, this is because legally it is a fairly complex area.

4. Effective management of antisocial behaviour requires effective sharing of information amongst authorities. Ministers are determined that unnecessary obstacles to the sharing of that information are eliminated.

5. Section 139 of the 2004 Act makes specific provision on the disclosure and sharing of information to help facilitate exchange of information where this is necessary or expedient for the purposes of any provision of the Act, or any other enactment the purpose of which is to make provision for or in connection with antisocial behaviour or its effects.

6. This guidance is intended to help explain the effect of the provisions in the 2004 Act and how they relate to other rules of law on sharing of information. It also provides good practice guidance on disclosure and sharing of information for practitioners dealing with antisocial behaviour.

Contact

7. If you have any queries about this guidance please contact the Antisocial Behaviour Unit on 0845 774 1741 or e mail: antisocialbehaviourunit@scotland.gsi.gov.uk

8. In addition, as part of the wider programme of support for the implementation of the Antisocial Behaviour etc (Scotland) Act 2004, the Executive is funding a telephone advice line for practitioners. The service will provide telephone advice and support on a wide variety of technical issues such as how to apply for an Antisocial Behaviour Order, the process of granting a closure notice etc. This service will be available from the end of November 2004 and the number will be widely published in advance. If you want to find out more information about the advice line, you can contact the Executive's Antisocial Behaviour Unit by email at: antisocialbehaviourunit@scotland.gsi.gov.uk

WHO IS THIS GUIDANCE FOR?

9. First and foremost, this guidance is for people in “relevant authorities” who might have to disclose or share information to deal with, or prevent, antisocial behaviour. For the purposes of the legislation, a “**relevant authority**” is:

- a local authority
- a chief constable
- the Principal Reporter
- a registered social landlord
- an authority administering housing benefit; and
- a person providing services relating to housing benefit to, or authorised to discharge any function relating to housing benefit of a local authority or an authority administering housing benefit.

The interpretation of “relevant authority” is provided as section 139(5) of the 2004 Act. A registered social landlord means a body registered in the register maintained under section 57 of the Housing (Scotland) Act 2001.

10. Secondly, this guidance is of relevance to those working in the voluntary sector and other professionals, such as health professionals who might be asked to provide information to assist persons fulfilling functions under the 2004 Act, or under other legislation which aims to deal with antisocial behaviour and its effects. In particular, section 139 and this guidance may have implications for persons who are susceptible by virtue of any enactment or rule of law to a sanction or other remedy, if the information they are responsible for is sought under the 2004 Act by a relevant authority. Guidance on the relationship to other rules of law is provided below.

11. Section 139(6) provides that any person who, by virtue of the 2004 Act, must or may provide information or who provides or receives information for the purposes of any provision of the 2004 Act shall **have regard to** any relevant guidance given by the Scottish Ministers. While other guidance documents on sharing of information may also be relevant, practitioners working to deal with antisocial behaviour should have regard to this document.

WHAT DOES THE ASB ACT PROVIDE ON SHARING INFORMATION?

12. Section 139 of the 2004 Act makes specific provision on the disclosure and sharing of information to help facilitate exchange of information where this is necessary or expedient for the purposes of any provision of the Act, or any other enactment relating to antisocial behaviour or its effects.

13. This section is based on a similar provision at section 115 of the Crime and Disorder Act 1998 which applied to provisions in the 1998 Act, including applications for an antisocial behaviour order and proceedings for eviction on the grounds of antisocial behaviour.

14. Section 139 provides a legal protection for those who disclose information where the disclosure of information is necessary or expedient for the purposes of any provision of the 2004 Act, or any other enactment the purpose of which is in connection with antisocial behaviour or its effects. This would include, for example, individuals sharing information to support the preparation of antisocial behaviour strategies or preparing to apply for an antisocial behaviour order or pursuing an eviction on grounds of antisocial behaviour, under the Housing (Scotland) Act 2001. However, a person disclosing information and relying on this protection will have to be satisfied they are complying with the Data Protection Act 1998 and any other relevant rules of law.

15. Where a person discloses information to a relevant authority under section 139 which is subject to a duty of confidentiality, and where they inform the authority of the breach of that confidentiality on disclosing the information, the authority must respect that confidentiality and shall not disclose the information. The exception to this is in cases where the disclosure is permitted or required by law. For example, there is a duty to co-operate with a local authority making enquiries under section 21 of the Children Act (Scotland) 1995.

16. The provision at section 139 is not the only part of the 2004 Act which relates to information exchange. For example, Part 1 on antisocial behaviour strategies makes clear that local strategies should include material on exchange of information between the local authority and the police relating to antisocial behaviour. In addition, sections 14 and 15 make provision on information and records relating to antisocial behaviour orders.

17. Operationally, section 139 is the most significant provision on information sharing as it impacts on every part of the Act and other pieces of legislation which relate to antisocial behaviour. It is of particular relevance to authorities using powers under the Act, such as the power to apply for an antisocial behaviour order or a parenting order. Section 139 facilitates the disclosure and sharing of information to deal with antisocial behaviour by providing a clear, statutory justification. A lack of statutory underpinning can undermine efforts to adopt practical arrangements on information exchange. A statutory reference point such as that provided by section 139 can prove helpful in providing legal authority, where there is a reasonable case to disclose.

HOW DOES THE ASB ACT RELATE TO DATA PROTECTION AND OTHER LAW?

18. Any person disclosing information and relying on the protection provided by section 139 of the Antisocial Behaviour (Scotland) Act will have to have regard to the potential applicability of the Data Protection Act 1998 and any other relevant rules of law. The law on information sharing is relatively complex and there has been confusion over what can be done legitimately. Essentially, a balance has to be struck between rights to privacy and the need to take legitimate steps to protect the community from crime and disorder.

19. This guidance will not explain in detail the implications of the Data Protection Act, human rights legislation and other relevant rules of law, but should help promote good practice in information exchange to tackle antisocial behaviour. Every case is different and no guidance document on disclosure and sharing of information will remove the need for decisions to be made which are reasonable and proportionate. Legal advice should be sought where there is any doubt in a particular case.

20. Firstly, it is important to emphasise that the law sets a framework for legal information sharing and provides safeguards for individuals against unauthorised use of personal information that infringes their privacy. It does not prevent agencies from developing joint, cooperative working arrangements to enable information to be shared quickly and efficiently whenever it is necessary and appropriate to do so. You may find it helpful to refer to the Executive publication, "Data Sharing: Legal Guidance for the Scottish Public Sector", which provides information on relevant legal issues to lawyers and to other interested professionals working in the public sector. This is available at:

<http://www.scotland.gov.uk/about/FCSD/21stCG/00018836/page1773973958.aspx>.

The Data Protection Act 1998

21. Misunderstanding about the Data Protection Act 1998 ("the DPA") has caused a great deal of confusion and uncertainty about the circumstances in which data may be shared. It is a complex area of law and if in doubt you should seek guidance from your lawyers or your organisation's Data Protection Officer.

22. The Data Protection Act 1998 was enacted to give effect to the principles contained in a European Directive¹. The objective of that Directive is to ensure that states "*protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.*"

23. The Act sets out a framework of controls over the way in which data relating to individuals from which they can be identified can be used. It does not affect the sharing of other information. There are many situations in which personal data can be used and disclosed **and it is a mistake to think that the DPA always prevents**

¹ EC Directive 95/46.

you from using or sharing data if you do not have the person's consent. There are many other situations in which you can disclose information covered by the DPA.

24. The first principle of the DPA is that data must be processed fairly and lawfully. The Act expands on this principle as it sets out conditions that must be met for the lawful processing of personal data (the Schedule 2 conditions) and additional conditions that must also be satisfied for processing sensitive personal data (the Schedule 3 conditions). These are wide ranging and include fulfilment of a statutory duty or function of a government department or of the Crown. In all cases the processing must be necessary² to fulfil these purposes. If what you want to do is covered by a Schedule 2 condition (and a Schedule 3 condition for sensitive personal data) and you follow the 8 principles you will be acting in accordance with the DPA.

25. It must be remembered that Data Protection failures will lead to a loss of trust and hinder the very purpose of protecting communities. Following the basic steps to ascertain the legality, necessity and proportionality of processing personal data should ensure that such an outcome is avoided. Full legal guidance on the Data Protection Act 1998 is available from the Information Commissioner's website at www.informationcommissioner.gov.uk

Misconceptions about data protection law

26. Over the years several misconceptions in relation to data protection have been presented as facts. In some quarters these have become accepted as accurate interpretations of existing data protection legislation. Examples of them are cited below.

(a) *"Data Protection prohibits sharing personal information."*

27. The Data Protection Act 1998 set out to ensure that the various personal databases operated by public and private sector agencies, which often contain sensitive personal information, are not used to disclose this information without lawful purpose, where there is no wider public interest, or where sharing is clearly unreasonable.

28. A company passing on customer details to another private sector business to assist their marketing is clearly outwith the law while the example of a public space CCTV organisation allowing publication of an image identifying an individual intending to commit suicide has been held to be unjustified and disproportionate.

² Detailed guidance on how to determine what is necessary is to be found in the guidance on the DPA issued by the Information Commissioner – available on his website at www.dataprotection.gov.uk.

29. Disclosing personal data is legal where:

- the purpose of the disclosure is directly related to an explicit or implied duty of an agency, (for example the police providing a Registered Social Landlord with information on a complaint of antisocial behaviour to enable them to apply for an ASBO against a tenant or visitor to the house as a means of preventing disorder or the RSL providing similar information to the police to enable them to prepare a report to the Procurator Fiscal for consideration of prosecution as a means to fulfil its duty of care to other residents) or where there is either a statutory duty or power to disclose;
- the processing conforms to or is exempt from the Data Protection principles and it is deemed necessary to achieve the legal purpose.

(b) *“A cautious approach is the safest approach.”*

30. There has also been a tendency to emphasise the risks associated with disclosure while minimising or even denying the possibility of risk in non-disclosure. Though the lessons to be learned from Soham and the resultant Bichard Inquiry are complex it is clear that when assessing the balance of interests between sharing and not sharing it can no longer be assumed that the cautious approach presents the safest option. Routinely erring on the side of non-disclosure offers much less chance of achieving a safe outcome than professional judgement.

(c) *“Sharing information infringes individual’s rights.”*

31. Unless freely consented to, disclosure will always involve some infringement of a person’s right to privacy. It is wrong to assume, however, that disclosure may not actually assist the person concerned or those affected by their behaviour to justify disclosure. For example, where an application for an antisocial behaviour order is being considered, there may be social or mental health issues present which, if known, would result in less formal action being taken in support of the individual. Disclosing information to relevant authorities, who would have to respect the confidentiality of the information, could be of benefit to the individual concerned as it could increase understanding of their circumstances and influence the approach taken by the authority in seeking to prevent further crime and antisocial behaviour.

32. Instead of legal action being taken specialist support may be provided which is more appropriate in the circumstances of the case. For health professionals and others it is important to recognise that personal information, shared legitimately bearing in mind relevant rules of law, can be viewed in a positive light as something which will be of benefit to that individual. This example is not intended to negate principles around confidentiality but to remind that disclosure should always be based on individual circumstances and consideration of the wider interest. The common law duty of confidence – which is discussed later in this guidance - may also be of relevance in such cases.

(d) *“With protocols we can now share all our personal information.”*

33. A number of protocols governing sharing arrangements between agencies in relation to antisocial behaviour can be found across the country. These have resulted from an awareness that public bodies must work together to tackle antisocial behaviour – both its symptoms and its causes - and must be able to provide guidance to staff on the:

- purpose/s of the protocol
- circumstances when sharing can be carried out
- procedures to be adopted when receiving requests
- the manner of storing the information and
- the key members of staff responsible for monitoring the implementation of the new arrangements.

34. This has led some to believe that any requests for information can be accommodated and that all personal information held by organisations should be disclosed. This is not the case. Professional judgement (bearing in mind relevant rules of law, protocols, exceptions, circumstances of case etc) has to be used to ensure that disclosure is legitimate and proportionate. It is also likely the signatories to the protocols will withdraw their support if protocols are used to justify inappropriate sharing of information.

35. It is not necessary, however, to have separate Protocols for separate purposes. One can cover two or more specified aims as long as each of the participating agencies has a legitimate interest in each of them and with the proviso that no information processed for one purpose should be processed for an incompatible purpose.

36. Advice regarding the creation of protocols is given below. The subject is comprehensively covered on the Department for Constitutional Affairs’ website at <http://www.dca.gov.uk/foi/sharing/toolkit/index.htm>.

(e) *“You can go to prison if you get it wrong.”*

37. There are statutory offences concerning the unauthorised access or modification of computerised material. Offences under the Data Protection Act relate to individuals knowingly or recklessly obtaining, disclosing, selling or offering to sell personal data. These offences generally arise where an individual deceives or misleads a data controller into providing them with personal data. There are other offences under the Data Protection Act relating to a data controllers’ failure to notify systems or comply with enforcement notices. The Computer Misuse Act 1990 lists the relevant offences relating to deliberate and unauthorised acts such as passing on Police National Computer information for financial reward.

38. The consequences of a data controller breaching the Data Protection Principles during the course of a data sharing exercise are that the relevant authority may be served with an Enforcement Notice requiring them to take steps to remedy that breach. Although a breach of the Principles is not an offence, a breach of notice

is. It is important to note that such action can only be taken against the data controller and not individual employees of the authority.

The Human Rights Act 1998

39. The Human Rights Act 1998 (“the HRA”) imposes a duty on public authorities to act in accordance with the “Convention rights” contained in the European Convention on Human Rights that are listed in the Act. (These are set out in Schedule 1 to the HRA). This duty affects the way in which all public bodies carry out their functions. If you work for a local authority, the NHS, a government department or agency, the HRA applies to everything that you do. If you work for a private company, a charity or a voluntary organisation that carries out some functions on behalf of public authorities, the HRA also applies to you when you are doing that work.

40. In practice, if you follow the 8 data protection principles it is likely that you will also comply with the requirements imposed by the HRA.

Article 8.1 states:

“Everyone has the right to respect for his private and family life, his home and his correspondence”. When you are dealing with information concerning individuals you must act in ways that are compatible with this right. As with many Convention rights, the right is qualified,

Article 8.2 states:

*“There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, **public safety** or the economic well-being of the country, for the **prevention of disorder or crime**, for the **protection of health or morals**, or for the **protection of the rights and freedoms of others**.”*

41. If you seek to rely on one of the grounds in Article 8.2 for interfering with an individual’s right to respect for private life, you must act with “proportionality”. Article 8.2 does not give you ‘carte blanche’ to ignore the right to respect for family and private life. You have to balance the competing interests, and if you have to infringe the right you must try to minimise the infringement to the person’s right when seeking to achieve your wider public interest goals.

42. There are of course many circumstances where the fact that someone’s right to privacy would be infringed must not be allowed to prevent you from taking appropriate action. It is important to remember that one of the qualifications to this right is the prevention of disorder or crime. More detailed guidance upon Article 8, including discussion of some of the most important case law, has been published by the Department for Constitutional Affairs. <http://www.dca.gov.uk/hract/guidlist.htm>

43. It should also be remembered that disclosure can assist in protecting other individuals’ rights, most notably:

- Article 2 - the right to life
- Article 3 – the right not to be subject to torture or to inhuman or degrading treatment
- Article 5 – the right to liberty and security of person
- Article 9 – the right to freedom of thought, conscience and religion
- Article 11– the right to freedom of peaceful assembly and to freedom of association with others
- Article 14- prohibition of discrimination
- Article 17 – prohibition of abuse of rights

44. Agencies should not over-emphasise the rights of offenders over the rights of victims.

The Common Law Duty of Confidence

45. As a general principle the duty arises when a person receives information in circumstances where he knows or can be taken to know that the information is to be treated as confidential. For example, NHS patient information is nearly always under a common law duty of confidence. Whenever you obtain information in circumstances where a duty of confidence is to be inferred, you have a legal duty to respect the confidentiality of information provided to you and not to disclose it to third parties without consent, unless an overriding public interest requires it. Under common law you have a duty to act reasonably and in a manner that is proportionate to your aim.

46. Often the common law duty will be reflected in statutory provisions and it is overridden by any express statutory duty to disclose information, for example to help in the detection of crime or to prevent serious harm to a child. This includes for example the duty to co-operate with a local authority making enquiries under section 21 of the Children Act (Scotland) 1995. The duty under sections 94 and 95 of the Sexual Offences Act 2003 also overrides the common law duty of confidence.

47. Generally speaking, you will satisfy your legal obligations under the common law duty of confidence if you handle personal data in a manner that complies with your obligations under the DPA.

48. One public body can sometimes justify disclosure of information that is subject to a duty of confidence to assist another public body in performing its public functions. However, the application of this defence is limited, and guidance should be sought from your legal adviser as to its relevance in every case.

49. The established categories of public interest that might override the common law duty of confidence are:

- The protection of health and morals
- Public safety
- The prevention of crime and disorder
- The protection of the rights and freedoms of others
- National security
- Economic well being of the country

50. In deciding whether or not disclosure of information given in confidence is justified you need to weigh the harm that might result if you fail to disclose the information against the harm that would result from breach of confidence. The disclosure must be proportionate and the minimum necessary to achieve the public interest objective. If you have to disclose information that was obtained in confidence you should always record in writing that the information was disclosed without consent and the nature of the public interest justification.

51. Considerations to take into account when determining issues of public interest are:

- The proportionality of disclosure
- Impact on or benefit to offender
- Impact of non disclosure on victim
- Disclosure supporting rights and freedoms of other individuals and
- Necessity of disclosure to achieve aim.

PROTOCOLS

52. Information sharing protocols can greatly assist authorities working to deal with antisocial behaviour. They help establish a framework for good practice in the disclosure and sharing of information to help agencies prevent crime and disorder while fulfilling obligations in respect of data protection and other relevant rules of law.

53. Any protocol must address the following matters:-

- A definition of the matters which will be included within the protocol.
- List the organisations involved in sharing data.
- Describe what they each/all do.
- The legislative basis for sharing information.
- Identify those officers who are responsible for ensuring compliance.
- Identify the information which officers are authorised to exchange.
- The method of exchange for information, including for urgent cases.
- A system for recording requests and action upon them.
- Methods of ensuring that information is held securely.
- Realistic timescales.

State the reasons for data sharing eg:

- To co-operate on a joint strategy for tackling antisocial behaviour.
- To tackle individual cases of antisocial behaviour.
- To collect statistical information to analyse trends.
- To contribute to research and evaluation.
- Explain how the accuracy of shared information will be maintained and partners are informed if inaccuracies come to light.
- Establish how complaints touching more than one of the partners will be dealt with.
- Indicate how staff training to promote awareness of responsibilities in relation to the protocol will be conducted.
- Build in regular reviews of procedures relating to the protocol.

54. The protocols between some RSLs, local authorities and police forces allow for the pro-active supply of information relating to criminal activity where the tenancy is integral to the activity so the RSL or local authority is alerted to the activity and can take action against the tenant. This is most often but not exclusively in the case of drug dealing. Where such protocols are operated consistently they can make a distinct impression on antisocial behaviour in an area and are very helpful to RSLs and local authorities.

Requests to disclose and share information

55. Local authorities, chief constables, registered social landlords, the Principal Reporter and authorities administering housing benefit make up the current definition of 'relevant authorities' under section 139 of the Antisocial Behaviour etc. (Scotland) Act 2004. Officers will have to consider requests to disclose or share information to help prevent crime and antisocial behaviour or to fulfil other roles under the 2004 Act. Requests may be in the context of a legal action such as an application for an antisocial behaviour order or an eviction or to support a voluntary measure such as an acceptable behaviour contract. Authorities will feel most confident in sharing information in respect of action which is clearly underpinned by legislation. For example, an ASBO application, backed up by the provisions at section 139 of the 2004 Act.

56. It is important to remember that section 139 applies to the whole of the Antisocial Behaviour Act, and other legislation which deals with antisocial behaviour and its effects. This means that it includes disclosure and sharing of information to support antisocial behaviour strategies under Part 1 of the Act. Strategies deal with prevention and early intervention as well as legal measures. It would, for example, be legitimate to share relevant personal information with relevant authorities to support the drawing up of an acceptable behaviour contract (ABC) to prevent further crime and antisocial conduct, despite ABCs being a voluntary agreement. The information should be relevant and if there are sensitive issues, it may be more appropriate to refer matters to the Children's Reporter. Where information is being shared to carry out an assessment of antisocial behaviour in the local authority area non-personal information should be used.

57. It is also important to be aware that section 139 also assists the sharing of information to promote the welfare of children as it applies to all measures in the Act, including parenting orders and the provisions on local authority accountability at sections 136 and 137.

Requests from the police

58. The police are responsible for the investigation and detection of crime and for apprehending of offenders. Information collected for the purposes of the prevention, investigation or detection of crime and the apprehension or prosecution of offenders is exempt from the principles of the Data Protection Act 1998 by section 29 of that Act. This means that the RSL or local authority must disclose all relevant information held by them to support any of the above police activities.

59. However, the RSL or local authority should also act pro-actively and where staff receive a report or witness antisocial behaviour whose nature makes it suitable for referral to the police, this should be done. The onus will be on each party to the protocol to ensure that confidential information is protected against unauthorised disclosure.

Requests to the police

60. Where action is being taken against an individual to prevent further antisocial conduct (whether the action involves legal process such as an ASBO or a voluntary agreement such as an ABC), the police should disclose to relevant authorities information in relation to:

- Relevant charges and convictions recorded on SCRO (Scottish Criminal Records Office) or PNC (Police National Computer);
- Police warnings;
- Details of police attendance and call outs (command and control logged incidents) relating to relevant offences;
- Information on conduct which may not have amounted to a criminal charge after police investigation. For example, an individual who calls out the police would be defined as a person who has been caused alarm or distress unless the call has been found to be of a malicious nature.

61. Relevant information on antisocial behaviour will include any criminal offence which has caused or could in all likelihood have caused alarm or distress.

For example:

- vandalism,
- theft,
- assault,
- breach of the peace,
- noise offences,
- wilful fire raising,
- theft of a motor vehicle,
- driving without a licence,
- driving whilst under the influence of alcohol have all been deemed to fall within the definition.

Please note, this list is not exhaustive or prescriptive.

62. Relevant authorities should also consider the relevance of the information in respect of the spatial context of the antisocial behaviour and the type of action being considered. For example, a registered social landlord can only apply for an ASBO in relation to a person in, or likely to be in, a property or the vicinity of such a property provided or managed by that landlord. Information should be relevant in some way to the application. This is similar to the provisions in the Housing (Scotland) Act 2001 in respect of eviction proceedings. The local authority or registered social landlord can take action to evict a tenant on the grounds that the tenant, a person residing or lodging in the house with the tenant or a person visiting the house has been convicted of an offence punishable by imprisonment committed in, or in the

locality of the house. *Locality* includes the wider neighbourhood. For example convictions or charges relating to behaviour within a radius of one or two miles of the house may be relevant, though convictions for behaviour in the city centre will not be relevant for a person residing in the suburbs in respect of an application for eviction. This specific location of the incidents will be of less relevance where action is being taken to protect the wider community.

63. Where a robust protocol is in place, trust will be engendered in all parties which will enable more informal or urgent approaches to be made. For example, when handling pre-application requests for disclosure. Information may be exchanged prior to the commencement of legal action for eviction or an antisocial behaviour order. The less formal information gathering exercise will allow the local authority and the police to establish whether there is sufficient justification for legal proceedings, without the need for a formal application at an early stage. This will avoid unnecessary time consuming requests.

CONCLUSION

64. Data sharing constraints hamper agencies in utilising legislation designed to assist in combating antisocial behaviour and disorder and frustrate many of those involved. Resolution or amelioration of this problem should result in more robust and speedy responses, more effective joint working and safer, more secure communities.

65. It is important that knowledge of data protection issues, relevant guidance and good practice is shared widely. This guidance does not provide all the answers, but chief officers are strongly encouraged to take active steps to promote sharing of knowledge and good practice on the disclosure and sharing of information to help prevent crime and antisocial behaviour.

Protocols are living documents. As such, they are always susceptible to the changes in law and best practice and should be updated and amended accordingly.

This model is a guideline only: users can tailor it to meet their own needs. Further useful information on protocols can be obtained from <http://www.crimereduction.gov.uk/infosharing21.htm> from which this protocol is adapted.

Contents are likely to include the following:-

1. Title Page
2. General Introduction
3. Undertakings
4. Non-personal Data
5. De-personalised Data
6. Personal Data
7. Designated Officers
8. Process of Information exchange
9. Security and Data Management
10. Complaints and Breaches
11. Audit
12. Signatories page
13. Glossary to the Protocol

1. TITLE PAGE:-

Protocol and Procedure for Exchange of information, as agreed between [Insert all parties to the protocol here].

Insert date of protocol at foot of page.

2. GENERAL INTRODUCTION

1. **Purpose:** The purpose of this protocol is to facilitate the exchange of information pursuant to the power contained in Section 139 of the Antisocial Behaviour etc. (Scotland) Act 2004. Section 139 enables any person to disclose information to a relevant authority where disclosure is necessary or expedient for the purposes of any provision of the Act **or any other enactment relating to antisocial behaviour or its effects** where that person would otherwise not have the power to disclose the information or would be, by virtue of any enactment or rule of law, susceptible to a sanction or other remedy if the person disclosed the information.

2. By signing this protocol, we declare our commitment to the procedures it sets out. The manner in which information can be exchanged takes into account the following legislation:
 - a. **The Data Protection Act 1998**, for the processing of personal information.
 - b. **The Human Rights Act 1998**, for the rights of the individual's privacy.
3. The scope of this Protocol is to clarify as far as is possible, under which circumstances information can be exchanged. We believe that a single, joint approach to exchanging information, is a highly efficient mechanism for reducing crime, disorder and antisocial behaviour.
4. It is the purpose of this Protocol, to clarify the understanding between [inset names of parties], on each party's responsibilities and duties towards each other. We are fully aware of the process for information exchange and will comply with all legal requirements.
5. All technical terms and abbreviations, are defined in the extensive Glossary section.
6. This Protocol will be published and made available to the general public, for clarity of purpose. Arrangements for dissemination of the protocol and steps being taken to raise awareness of the protocol will be explained in the protocol.
7. This Protocol is due to be next reviewed on [insert date], and any comments should be sent to [insert name of Primary Designated Officer (see glossary) and address.]
8. Any partner may withdraw from this Protocol upon giving written notice to the other signatories. Data which is no longer relevant should be destroyed or returned. The partner must continue to comply with the terms of this Protocol in respect of any data that the partner has obtained through being a signatory.
9. We agree no exchange of information especially personal information, should take place until each and every party to the exchange has signed up this Protocol

3. UNDERTAKINGS

1. As parties signed-up to this Protocol, we recognise the importance of sharing information with each other, in line with the aims of the Antisocial Behaviour etc. (Scotland) Act 2004 for the purpose of reducing crime, disorder and antisocial behaviour.
2. Parties in this Protocol undertake to co-operate fully with each other, within the parameters of the Data Protection Act 1998, the Human Rights Act 1998

and the Antisocial Behaviour etc. (Scotland) Act 2004, and in accordance with Scottish Executive and other government guidance associated with these Acts.

3. We pledge to periodically consult with each other upon matters of policy and strategy.
4. We undertake in this Protocol that where possible and appropriate, information requested in the correct manner (see process section), is given within a time limit of [to be agreed] days; this may vary depending on the nature, volume of requests and operational need.
5. Each partner pledges that all personal data remains the property of the disclosing agency, and is the responsibility of the data controller as defined by the Data Protection Act 1998.
6. Each party undertakes to ensure that it complies with all relevant legislation, this Protocol, and its internal policies on **disclosure**. Parties are recommended to seek their own legal advice, wherever necessary.
7. We agree to disclose information to [insert names of parties] who are relevant authorities or who are acting on behalf of a relevant authority for the purposes of the Act. Where the recipient is acting on behalf of a relevant authority, this means in their capacity as persons selected by the relevant authority to formulate or implement the crime and disorder or antisocial behaviour strategy.
8. We undertake to ensure that officers who have responsibilities relating to this protocol have sufficient training on an ongoing basis to reflect any changes in legislation or relevant guidance.

4. **NON-PERSONAL DATA** (optional)

1. We understand that non-personal data constitutes data that has never referred to individuals. Non-personal data is more often than not aggregate data. [see glossary]. It is non-personal data (never has referred to an individual) or aggregated data (derived from personal, non-personal and de-personal data), that is normally used for mapping. We can use this non-personal data for incidence or “hot-spot” mapping purposes.
2. We agree that non-personal data held by us may be subject to the provisions of the Freedom of Information (Scotland) Act 2002. We have the legal duty to provide non-personal data to a third party, if a formal request is made.
3. We will disclose non-personal data for the purpose of profiling local areas for antisocial behaviour activity, and to calculate the cost, scope and scale of proposed reduction interventions by parties to this protocol.

5. DEPERSONALISED DATA (optional)

[This type of data is seen as a good method for exchanging the information required, as long as this can achieve the required objective].

1. We accept that depersonalised data is used in the vast majority of antisocial behaviour audit activity, as management teams and analysts do not require personal data. Depersonalised data is excellent for profiling local areas, and in calculating the scale, scope and cost of proposed anti social behaviour interventions.
2. We understand that depersonalised data encompasses any information that does not and cannot be used to establish the identity of a living individual, and has had all personal identifiers removed. We note that the Information Commissioner has stated that even a post-code or address can give away the identity of an individual, if there is only one person living there
3. We accept there are no legal restrictions on the exchange within this Protocol of depersonalised data, although a duty of confidence may apply in certain situations, or a copyright, contractual or other legal restriction may prevent the information being disclosed to partners.
4. We appreciate that if several sets of depersonalised data were merged or compared with each other, there is a risk that an individual could be identified. We will always hold depersonalised data securely and destroy it securely, when it is no longer required.

6. PERSONAL DATA

1. We understand that personal data is information which relates to a living individual who can be identified from the data; this data will be clearly marked as personal data and kept securely within a pass-worded computer system or otherwise physically secure with appropriate levels of staff access. We undertake to destroy all personal data when we are sure that it is no longer required.
2. We undertake to formally record all grounds for disclosure of personal data. We will process data fairly and objectively for each case. We agree that we will only disclose sufficient information to enable our partners to carry out the relevant purpose for which the data is intended. This we will determine on a case by case basis.
3. Personal data should only be shared in a particular case when we, as the disclosing partner, are satisfied that: (a) We are legally empowered to do so. The conditions of schedule 2 of the Data Protection Act 1998 must be satisfied. (b) The proposed disclosure of personal data can be done in accordance with the principles of the Data Protection Act 1998 (c) We can disclose personal information reflecting the common law of confidentiality and the principles of the Human Rights Act 1998.
4. **Section 139 of the Antisocial Behaviour etc. (Scotland) Act 2004 provides us with lawful power for disclosure where this is necessary or expedient for the purposes of any provision of the Act or any other enactment which aims to deal with antisocial behaviour and its effects.**
5. We will disclose personal data relating to a victim, informant or witness with the consent of the data subject. **We will also disclose information without consent where there is an overriding public interest in disclosure.** This will be to designated staff or posts to enable them to carry out their duties in the exercise of a public function.

We can also disclose on a case by case basis, for the following reasons (provided there is a lawful basis for disclosure, where there is a substantial chance that one of the following purposes would be prejudiced).

- a. to prevent or detect crime;
 - b. to apprehend or prosecute offenders;
 - c. if it is required by law (bulk disclosures are also normally allowed);
 - d. if the disclosure is registered with the Information Commissioner;
6. When disclosure is required, we agree to ensure that:
- a. the information is being processed lawfully: the information is being processed fairly;
 - b. the public interest is of sufficient weight to over-ride the presumption of confidentiality and to justify any interference with the right to privacy etc in Article 8 of the European Convention of Human Rights;

- c. a disclosure is necessary to support action under the Antisocial Behaviour etc. (Scotland) Act or other relevant enactments;
- d. any disclosure must have regard to specific statutory restrictions on disclosure.

7. We understand the Public Interest criteria, to include:

- a. the administration of justice;
- b. maintaining public safety;
- c. the apprehension of offenders;
- d. the prevention of crime, disorder and antisocial behaviour;
- e. the detection of crime;
- f. the protection of vulnerable members of the community.

8. **Human Rights Act 1998:** Article 8 of the Human Rights Act 1998 states that everyone has the right to respect for his private and family life, home, and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law and is necessary in a democratic society in the interests of:

- a. National Security
- b. Public Safety
- c. Economic well being of the country
- d. The prevention of crime and disorder
- e. The protection of health or morals
- f. The protection of the rights or freedom of others

9. **Proportionality:** If the disclosure of information will in some way restrict the rights of the data subject, we will consider the rule of proportionality. This is to ensure that a fair balance must be achieved between the protection of the individual's rights, with the general interests of society.

10. **Use of information:** The second Data Protection Principle states that personal data may be obtained "for one or **more** legal purpose and shall not be processed in any manner incompatible with that purpose or purposes". This allows for information utilised for a criminal prosecution to be further adduced to support civil processes such as an ASBO.

7. DESIGNATED OFFICERS

1. We understand that each partner must appoint a Primary Designated Officer (PDO see glossary), who will be a Manager of sufficient standing, and have a co-ordinating and authorising role. We may also appoint further Designated Officers (DOs) within the same body.
2. The following named individuals are designated as PDOs to assume responsibility for data protection (including notification where appropriate), security and confidentiality, and compliance with all relevant legislation:

NAME	POST	ORGANISATION
[Insert name]	[Insert position]	[Insert name of party to protocol]

3. Our specific responsibilities will be the following:
 - a. Making sure the [named] party abides by the sections of this Protocol.
 - b. Ensuring that all DOs and other staff are fully aware of their responsibilities.
 - c. Appointing other staff in the body to act as DOs in their absence.
 - d. Authorising [named party's] involvement and co-operation in the information sharing process, at every stage.
 - e. Keeping a Protocol Co-ordination Folder, which holds all the partner's information sharing documents in general.
 - f. Ensuring [named party's] Data Protection Notification entry is accurate, up to date and adequate for the purpose for which it is intended.
4. [The appointment of the PDO needs to be confirmed in writing and stored on the Protocol Co-ordination Folder, for all partners to see].
5. Only DOs and PDOs of [named parties] can make the formal requests and document agreements for the sharing of personal information. PDOs and DOs can decide (on a case by case basis), why a disclosure is necessary to support action under the Act. We will also decide why and when the public interest overrides the presumption of confidentiality.
6. It is our responsibility to ensure that processing of the personal data held, is in keeping with the principles of the Data Protection Act 1998. These are, in summary form, that the data is:
 - a. Obtained, processed and disclosed fairly and lawfully.
 - b. Kept securely.
 - c. Processed in accordance with the rights of the data subjects.
 - d. Accurate, relevant and held no longer than necessary.
 - e. Disclosed only for a specified related purpose.
 - f. Disclosed without the subject's knowledge and/or agreement only where failure to do so would prejudice the objective.
7. We [name] PDO or DO are the data controllers. As such, any final decision or whether to share sensitive information, rests with us.

8. PROCESS

1. Signatories to the Protocol will define the requirement, outline the nature of the risk, identify the information holders and agree future disclosure procedures. It is this initial contact between us whether by meeting, correspondence or telephone, that is fundamental to the drawing-up of this Protocol. **This process may involve meetings, but the process must be documented in writing. This is to provide a paper trail for any audit and for clarity purposes.**
2. Agreed disclosure procedures will generally require making a request in writing. The reply to this request will normally be made within [insert timeframe]. As the disclosing partner, it is my responsibility to make the assessment and consider the nature of the formal request, replying within [Insert time-frame]. Specific provision should be made on the handling of urgent cases.
3. Access to personal information by staff other than PDO or DOs, should be limited to employees whose work is directly related to the requirement for disclosure.
4. The data subject is legally entitled to request their records from the receiving agency unless an exemption under the Data Protection Act 1998 applies. If the subject requests access to their records, PDO or DO should immediately contact the disclosing agency, to determine whether the latter wishes to claim exemption. From this stage, the procedure should be fully documented in writing and stored on file.
5. We must agree the criteria for the review and weeding of data in accordance with existing policies and codes of practice [insert here]. This should cover variations of data held by us and we should agree a maximum retention period for each item of data.

[It must be noted that the above represents the recommended approach to setting-up data sharing arrangements. You may have less formal arrangements.]

9. SECURITY AND DATA MANAGEMENT

1. It is our responsibility as signatories to this Protocol, to ensure that we have adequate security arrangements in place, in order to protect the integrity and confidentiality of the information we hold.
2. We agree that personal information disclosed must:
 - a. Not be e-mailed over internet links, without adequate security being in place (e.g. use of a secure network such as the Government Secure Intranet).
 - b. Be protected by back-up rules.
 - c. When stored on a computer system, it must be password protected and we agree this password will be revised regularly.
 - d. When manual, be stored in a secure filing cabinet when not in use.
 - e. Be located in a geographically secure environment.
3. All personal data disclosed to us will be held until the issue to which is related is resolved and no longer than necessary to achieve this. However consideration will always be given circumstances where it is necessary to retain certain types of information.
4. We understand that all these measures need to be taken to ensure the security of our partners and to protect the general public.
5. We are aware that only the minimum amount of information should be disclosed, in order to get the job done and not in a manner incompatible with the purpose or purposes for which the personal information was obtained. We agree that all information retained by us and our partners should be kept securely.
6. We undertake to explain how the accuracy of shared information will be maintained and partners are informed if inaccuracies come to light.

10. COMPLAINTS AND BREACHES SECTION

Complaints:

1. Initial complaints must be referred to the appropriate PDO or DO [insert names] and we agree in this Protocol, the procedure to be followed in the event of such a complaint being received, is as follows; [insert your agreed procedure].
2. We agree that any formal complaint by a data subject regarding any stage of the process will be notified (as a best practice measure) in writing to all of our partners.
3. We undertake to do all that we can within the guidelines of the Data Protection Act 1998, to assist with any complaint.
4. Individuals do retain the right to raise a complaint with such bodies as the Information Commissioner or the statutory Ombudsman.

Breaches:

5. We agree that any breach of confidentiality will seriously undermine and affect the credibility of our work, our partnership objectives, and may render us liable for breach of the law.
6. We undertake at all times, to comply with data protection and other legal requirements relating to confidentiality.

11. AUDIT

1. **Audit of Data:** We undertake to ensure that we will collect, process, store and disclose all data held by us, within the terms of this Protocol and the relevant legislation. We agree to ensure that all information held by us, is accurate, relevant and fit for the purpose for which it is intended.
2. **Audit of Security:** We agree to store all held data securely as per the terms of the Security and Data Management section. We will dispose securely of all data held. We also pledge to conduct six-monthly audits of our security arrangements, to ensure they are effective.
3. **Audit of Protocol:** We undertake to conduct regular audits of this Protocol at [state fixed periods here], in order to amend it and ensure it remains fully effective.

SIGNATORIES SECTION

This Protocol [insert title here], must be signed by a representative of sufficient standing from each of the named parties, in the following format:

AGREEMENT

SIGNED _____
[Type of Official-see below] For and on behalf of [named party] Date

SIGNED _____
[Type of Official-see below] For and on behalf of [named party] Date

[Repeat the above process until a representative from each named party on this Protocol is included].

[It must be noted that the Protocol should be written in as plain and clear English as possible].

[Insert as many terms as are relevant to your Protocol and / or add your own].

ACCESS LIST:	A register specific to a project where personal information is shared logging the authorised access to the information.
AGENCIES:	Those signatories party to this Protocol.
AGGREGATE DATA:	Data that consists of statistics of events forming a trend or pattern but from which it is not possible to identify individuals.
ANTISOCIAL BEHAVIOUR:	Acting in a manner or pursuing a course of conduct that causes or is likely to cause alarm or distress to at least one person who is not of the same household as the person engaging in the behaviour..
AUDIT:	A process of collating statistical data from lawful sources to identify trends or patterns in crime and disorder in order to formulate strategies and projects to disrupt and negate criminal and antisocial behaviour.
AUDIT TRAIL:	A process of collating data for the purpose of identifying and refining internal procedures of partner agencies, by means of examination of all documentation kept on the information exchange.
BULK TRANSFER:	The disclosure of a quantity/set of identifiable personal data, for the purpose of a criminal investigation/crime and disorder/ anti social behaviour initiative.
COMMON LAW:	A common law duty of confidentiality IS owed to the public. This requires that personal information given for one purpose cannot be used for another, and

places restrictions on the disclosure of that information. This duty can only be broken if the public interest requires it. Statutory provisions on disclosure override common law provisions.

CONSENT:

Agreement, either expressed or implied, to an action based on knowledge of what that action involves, its likely consequences and the option of saying no.

EXPRESS CONSENT:

Consent which is expressed orally, or in writing, (except where patients cannot write or speak, when other forms of communication may be sufficient).

DATA:

Essentially the same as "information" but tends to be information recorded in a form, which can be processed by equipment automatically (usually electronically), in response to specific instructions.

DATA IN THE PUBLIC DOMAIN:

Any information which is publicly available, whether it relates to a living individual or not. For example, information found on the internet, television or court records,

DATA CONTROLLER:

Is the person who decides the purposes for which and the manner in which 'personal data' is to be 'processed'.

DATA PROCESSING:

Includes the obtaining, holding, recording, retrieval, organisation and disclosure of data – it is a very wide concept indeed

DATA PROTECTION ACT 1998:

A major piece of legislation, governing who can store data and share it and under which circumstances. It embodies the eight basic principles of data processing, and gives guidance on data sharing.

DATA SHARING (EXCHANGE):

The physical exchange of data between one or more individuals or agencies; this is data recorded in an electronic or processing form. For example, this

usually involves the transfer of a data set to a partner agency.

DATA SUBJECT:

An individual who is the subject of personal data, being data from which a living individual can be identified.

DE-PERSONALISED DATA:

This is information where any reference to or means of identifying a living individual has been removed or “sanitised”.

DESIGNATED OFFICER:

A person nominated by the agency of sufficient standing, to process or initiate requests for personal information and data.

PRIMARY DESIGNATED OFFICER:

As Designated Officer, only the most senior member of the information sharing party in the partnership.

FORMAL REQUEST:

A written request by the Designated Officer for personal information made to the information holder.

HOT SPOT AREAS:

These are geographic areas of focus, where there is a disproportionately above average incidence of criminal activity and/or antisocial behaviour activity.

HUMAN RIGHTS ACT 1998:

This Act requires public authorities to comply with Article 8 of the European Convention on Human Rights, amongst other human rights. Article 8 is the right to respect for private and family life. Interference with this right is justified only when it is in accordance with the law, and is necessary in pursuing a legitimate public interest in a proportionate manner.

INDEMNITY:

Parties may seek to indemnify themselves against eventual legal action or litigation for compensation for damage or distress under the relevant legislation. As protocols are not legally binding documents it is wrong to assume that mention of an indemnity clause would place signatories beyond legal

challenge. We have thus omitted an indemnity clause in this model but it may be an option for an organisation (see section 37 above).

INFORMATION: This is essentially the passing of knowledge from one party to another in this Protocol.

INFORMATION SHARING (EXCHANGE): Involves a physical exchange of data between one or more individuals or agencies.

INTELLIGENCE: This is the end product of a process by which that information is checked and compared with other information and is then use to inform decision-making.

MAPPING: This is the process of combining data resources and the use of different types of data, to create a more accurate or clear picture of what is going on in the area.

NON-PERSONAL INFORMATION: Any information which does not or cannot be used to establish the identity of a living individual.

PERSONAL INFORMATION: Must relate to a living individual who can be identified from the data. Therefore, anonymised or aggregated data (see below) which cannot be used to identify particular individuals does not fall within the definition. Furthermore, personal data includes expressions of opinion and of the data controller's intention in relation to the data subject.

PERSONAL INFORMATION: Information which relates to a living individual who can be identified from the data or any other information which is in the possession of the data controller.

PROTOCOL CO-ORDINATION FOLDER: To be held by each partner agency giving an overview of its information-sharing arrangements.

PUBLIC DOMAIN:

Information is judged to be in the public domain when it is so generally accessible that it can no longer be regarded as confidential.

RELEVANT AUTHORITIES:

Any of these bodies or persons referred to in Section 139.

REVIEW:

Periodic review of data exchanged for the purposes of the protocol including review of the scope, relevance and accuracy of disclosed data; a review process which shall be defined at the time of the protocol initiation.

