

**The Clean Neighbourhoods and Environment  
Act 2005**

**“Working Together”**

**A Protocol for Parish, Town and Milton Keynes  
Councils and Thames Valley Police**

---

Section 1 Introduction .....	3
1.1 Background .....	3
1.2 Aims of the Protocol .....	3
1.3 Contents of the Protocol .....	3
1.4 New Powers for Parishes .....	5
1.5 Guidance for Parish Councils .....	5
1.6 What has been agreed so far? .....	6
Section 2 Mechanism for consultation .....	7
Section 3 - Information exchange .....	8
Section 4 - Standardised procedures .....	8
Section 5 - Coordinated response .....	9
Section 6 - Performance management .....	9
Section 7 - Training.....	10
Section 8 - Communications and publicity .....	11
Section 9 - Mechanism for a review process .....	11
Section 10 - Police Community Support Officers. (PCSOs). .....	11
Annex A. CNEA Working Together Group Terms of Reference .....	12
Purpose of Group .....	12
General Tasks .....	12
Membership .....	12
Lead Agency.....	12
Chair .....	12
The Vice Chair .....	12
Frequency of meetings .....	12
Administration .....	12
Annual Review.....	12
Annex B. CNEA Delivery Group Terms of Reference.....	13
Purpose of Group .....	13
General Tasks .....	13
Membership .....	14
Lead Agency.....	14
Chair .....	14
The Vice Chair .....	14
Frequency of meetings .....	14
Administration .....	14
Annual Review.....	14
AnnexC. Information Exchange Protocol.....	15

## **Section 1 Introduction**

### **1.1 Background**

Cleaner Safer Greener led to Clean Neighbourhoods and Environment Act given Parliamentary assent on 8<sup>th</sup> April 2005

1<sup>st</sup> Parish Council Seminar held Sept 05

Draft Guidance published Autumn 05

Working Group established

2<sup>nd</sup> Parish Council Seminar/Workshops February 06.

3<sup>rd</sup> Parish Council Seminar held July 2006

### **1.2 Aims of the Protocol**

The protocol will have the following aims:

- It will set out how Parish and Town Councils, Thames Valley Police and Milton Keynes Council will work together for implementation of the new powers of the Clean Neighbourhoods and Environment Act 2005 (CNEA).
- It will ensure the best use of resources within the Milton Keynes area.
- It will ensure that enforcement activity within Milton Keynes is fair, proportionate, consistent and equitable across the borough.
- The CNEA requires a consultative and coordinated response in dealing with environmental crime. The protocol will provide a framework for how the parties will work together to achieve this goal.

### **1.3 Contents of the Protocol**

The Protocol will be one of 3 key documents (the others being Policy and Procedures) and includes the following sections

- Mechanism for consultation
- Information exchange
- Standardised procedures
- Coordinated response

- Performance management
- Training
- Communications and publicity
- Mechanism for a review process
- Police Community Support Officers (PCSOs).

## 1.4 New Powers for Parishes

For the first time the CNEA will give Parish Councils a range of new powers to tackle some aspects of environmental crime. These are not duties, and Parishes can choose, which, if any of the powers they wish to enforce.

New powers include:

- Power to make a Dog Control Order
- Power to take an enforcement action against those that:
  - Commit an offence against a dog control order;
  - Litter;
  - Graffiti;
  - Fly Post.

The CNEA allows for the issue of Fixed Penalty Notices or provides the power of prosecution where a fixed penalty is not paid, or if the offence is deemed serious enough to go immediately to prosecution. The CNEA also gives some local discretion as to the level of the fixed penalty (within bands) and provides flexibility as to the amount of discount, if any, for early payment of the fixed penalty.

## 1.5 Guidance for Parish Councils

Defra has produced guidance for Parish Councils:

“Getting to grips with the Clean Neighbourhoods and Environment Act 2005 – a parish council guide to environmental enforcement”.

Copies of this can be obtained from:

Defra Publications  
Admail 6000  
London  
SW1A 2XX

Or it can be viewed on the Defra website:

[www.defra.gov.uk](http://www.defra.gov.uk)

or

<http://www.defra.gov.uk/environment/localenv/legislation/cnea/index.htm>

## **1.6 What has been agreed so far?**

A working group was set up which included Parish Councillor and MKC Officer representation from the Local Management of Community Safety Group, and the Anti Social Behaviour Group. A Workshop was held for all Parish Councils on 10 February 2006.

The following principles were agreed:

- That this protocol be developed between Milton Keynes Council and the Town and Parish Councils
- Fixed Penalties to be set at the default level, to be reviewed at a later date (after 6 months)
- Same Fixed Penalty Notice rates to apply across the Borough
- Same discounts to be offered for prompt payment
- MKC was to start the process in relation to a “blanket order” dealing with dog fouling.

## Section 2

### Mechanism for consultation

Implementation of the CNEA requires that consultation should take place between the bodies that are responsible for enforcing the Act, including those that may have chosen not to take up this power.

Consultation will ensure a fair and consistent approach across the Borough and avoid duplication. Key areas for consultation include the following:

- Dog Control Orders
- Level of Fixed Penalties (minimum set by Government)
- Level of discounts available to be applied.

Other areas, which will require discussion in the early stages of the process, include:

- Procedures
- Responsibility for ongoing prosecutions

All representatives of Town and Parish Councils, Thames Valley Police and Milton Keynes Council will meet annually as part of the “Working Together” group to review the protocol and address any issues which may have been raised during the year. A Chair will be appointed from within this group, and administrative support will be provided by MKC. **Terms of reference for the Working Together Group are attached as Annex A to this protocol.**

Operational issues will need to be addressed on a more regular basis, and there will be a need to constantly review the policy and procedures in light of best practice and any new legislation, which may be produced. To address this, a delivery group will be set up and will consist of key MKC staff who are involved in delivering the CNEA, Thames Valley Police and Parish representation. The group will meet initially on a quarterly basis and will develop the policies and procedures, which will be formalised by the full group. **Terms of reference for the CNEA Delivery Group are attached as Annex B to this protocol.**

All participants may have their items raised at any meeting. Prior notification of items will ensure appropriate responses can be prepared wherever possible.

### **Section 3 - Information exchange**

Sharing of relevant information will ensure a coordinated and appropriate response across Milton Keynes. Often, offenders are persistent and may also be known to other partner organisations for similar offences. Therefore information exchange, or intelligence sharing, is vital. However, sharing of this type of information is subject to tight controls, and adherence to relevant legislation is key.

To facilitate this and to ensure that all parties are aware of their responsibilities in respect of information sharing, a separate protocol will be drawn up. This protocol will take into account the following:

- Data Protection Act 1998
- Crime and Disorder Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998

It is important to note that this does not mean that parties **must** share information; it only provides them with the legal basis upon which they can legitimately share information if the need arises.

Town and Parish Councils, Milton Keynes Council and Thames Valley Police, who wish to take up these powers, will be required to sign the Information Exchange Protocol, if they wish to share, or receive relevant information, **The Information Exchange Protocol is attached as Annex C to this protocol.**

### **Section 4 - Standardised procedures**

The parties will agree to adopt and follow the procedures as set out in the Procedures document. Borough wide consistency of approach and compliance with policy and procedures, such as for evidence gathering, is important if formal legal action is taken through the courts.

The mechanism for agreeing the procedures to be followed will be through the operational group as set out in Section 2.

## **Section 5 - Coordinated response**

The level of success in respect of implementing the CNEA, is dependant on a coordinated response across the agencies in Milton Keynes who agree to take up and implement these powers. This will avoid duplication as well as disproportionate and inconsistent action. Failure in any of these areas may be used as part of a defence in any resulting prosecution.

This response can be achieved through agreement to, and compliance with, this protocol and will be reinforced by the agreement to adopt the same levels of fixed penalties and discounts to ensure consistency across the Borough. The parties will also inform each other of the powers they intend to adopt or implement. A mechanism will be set up to allow Partners to share information about their activities to avoid duplication.

## **Section 6 - Performance management**

To help with performance management, agreed procedures will be set up on how performance information should be collected, and in what format. This will facilitate rapid information sharing and help in sharing Best Practice. The Information Sharing Protocol will set out how and in what format the information can be shared legally.

The parties will share information on the following:

- Numbers of Fixed Penalty Notices (FPN's) issued and for what offences
- Numbers of FPN's paid – both with the discount period and within the statutory period
- Numbers of FPN's not paid – together with information on the (proposed) follow up action
- Number of prosecutions – successful and unsuccessful
- Information on warnings, cautions or any other type of educational activity, which has not resulted in a FPN or prosecution.

## **Section 7 - Training**

The guidance for Parishes has stated that all officers working on behalf of the Parish Councils, except Police Community Support Officers (PCSOs) must attend a Government approved training course. This training is currently being provided by Encams and can be found on their website:

<http://www.encams.org/events/sub.asp?sub=11>

or by phoning on 01942 612 621

Ongoing training is important to keep officers up to date on the legislation and will also allow each officer to learn from the experience of others. The operational group will undertake to arrange additional training as required. This will ensure that a consistent & thorough training is provided. Funding for this training would be through the participating agencies. In addition, the operational group will hold a database of courses, to which officers have attended, and can recommend.

## **Section 8 - Communications and publicity**

Any enforcement activity should also include educating people on what the laws are, and what penalties there are for breaching those laws. This action may deter some people from committing these acts. Publicity is a powerful tool for educational purposes, and will be all the more powerful if it can be jointly agreed by all agencies. This does not mean that individual agencies cannot issue their own publicity, but only that agreement is reached on the message they wish to send out. This will ensure accuracy, and ensure that the same message is being sent across the whole of Milton Keynes.

Information should be shared on any campaigns which are being proposed, this will allow other agencies to join in and can help publicise the campaign across a wider area.

## **Section 9 - Mechanism for a review process**

Evaluation and review is an important part of any process. From this can be learnt what works well, and what does not.

The CNEA also allows greater flexibility on levels of FPNs and discounts allowable. For this reason, a review should be conducted at 6 months after the adoption of this protocol and implementation of the relevant parts of the Act and again after 12 months. The review process should include all agencies who can undertake the enforcement action, whether or not they have chosen to do so. This will ensure all agencies are kept up to date with the processes and can see what is involved.

## **Section 10 - Police Community Support Officers. (PCSOs).**

PCSOs are able to issue FPNs in relation to offences of littering, dog fouling and Graffiti.

They must be authorised by either Milton Keynes Council or by the relevant Parish Council for the area they are working. For a Parish to authorise the PCSOs, they will need to adopt the new powers, which includes taking on responsibility for any follow up legal action. They will adopt the procedures contained within this protocol.

## **Annex A. CNEA Working Together Group Terms of Reference**

### **Purpose of Group**

To ensure that Parish and Town Councils, Milton Keynes Council and Thames Valley Police work together for implementation of the new powers of the Clean Neighbourhoods and Environment Act 2005 (CNEA).

### **General Tasks**

1. Review the work of the delivery group and discuss the previous years achievements and issues.
2. Make recommendations to the delivery group as a result of the above discussions.
3. Raise awareness among Town and Parish Councils who currently are not undertaking enforcement action under the CNEA of the work being carried out.
4. Provide an opportunity for information exchange and sharing of best practice

### **Membership**

All Town and Parish Councils  
Milton Keynes Council  
Thames Valley Police

### **Lead Agency**

The Lead Agency will be Milton Keynes Council.

### **Chair**

The Chair will be elected by the group from one of the representatives.

### **The Vice Chair**

The Vice Chair will be elected by the group from one of the representatives and will be appointed 3 months prior to the meeting.

### **Frequency of meetings**

The group will meet annually.

### **Administration**

Officers of Milton Keynes Council will administer the meetings of the group.

### **Annual Review**

These Terms of Reference will be reviewed on an annual basis.

## **Annex B. CNEA Delivery Group Terms of Reference**

### **Purpose of Group**

- To ensure that Parish and Town Councils, Milton Keynes Council and Thames Valley Police work together for implementation of the new powers of the Clean Neighbourhoods and Environment Act 2005 (CNEA).
- The group will ensure the best use of resources within the Milton Keynes area.
- It will ensure that enforcement activity within Milton Keynes is fair, proportionate, consistent and equitable across the borough.

### **General Tasks**

1. Review and implement the Protocol, ensuring compliance by all signatories
2. Develop and implement Policy and Procedures, ensuring consistency of application and standardisation across the Borough.
3. Develop, implement and review the Information Exchange Protocol ensuring compliance by all signatories
4. Monitor the effectiveness of all training provided to staff, including the Government provided training for Parish staff.
5. Develop, deliver or monitor delivery of training courses, maintaining a database of recommended courses.
6. Ensure that consultation is carried out across all signatories to the protocol.
7. Ensure that all signatories collect data as agreed in the protocol.
8. The group will provide guidance to all agencies on all communication issues to ensure that an accurate and consistent message is being sent across the Borough.
9. The group will review the Protocol, Policies and Procedures 6 monthly for the first year (from April 06) and annually thereafter.
10. Report to the Working Together Group on an annual basis
11. Consider recommendations made by the Working Together Group

## **Membership**

The group shall consist of representatives from the following organisations.

Milton Keynes Council	4
Town and Parish Councils	4 (1 rural, 2 urban and 1 Town)
Thames Valley Police	1 (in respect of PCSOs)

The Milton Keynes Council representatives will be officers responsible for the delivery of the Clean Neighbourhood and Environment Act. Nominations for Town and Parish Councillor representation will be made through the Milton Keynes Council Community Liaison Team, who will if necessary, arrange an election. To ensure maximum coverage in the borough, one representative only will be allowed from any Town or Parish Council.

## **Lead Agency**

The Lead Agency will be Milton Keynes Council.

## **Chair**

The Chair will be elected by the group from one of the representatives.

## **The Vice Chair**

The Vice Chair will be elected by the group from one of the representatives.

## **Frequency of meetings**

The group will meet quarterly. A calendar of meetings will be provided, additional meetings will be arranged as necessary.

## **Administration**

The meetings of the group will be administered by officers of Milton Keynes Council.

## **Annual Review**

These Terms of Reference will be reviewed on an annual basis.

## Annex C. Information Exchange Protocol

---

# **Clean Neighbourhood and Environment Act 2005**

---

## Protocol and Procedure for the Exchange of Information

## Introduction

### **Purpose**

1. The purpose of this Protocol is to facilitate the exchange of information to allow effective delivery of the powers contained in the Clean Neighbourhoods and Environment Act 2005 (CNEA 2005). It will clarify, as far as is possible, under which circumstances information can be exchanged, and that all parties understand their responsibilities and duties towards each other.
2. No exchange of information, particularly personal information, should take place until each and every party to the exchange has signed up to this Protocol. A list of all partners signed up for this protocol will be provided.
3. The intention is that a single, joint approach to exchanging information will mean a highly efficient mechanism for delivery of the CNEA 2005 and prevent breaches of the law regarding keeping and sharing information.
4. All technical terms and abbreviations are defined in the Glossary section in Appendix A.

### **Review**

5. This Protocol is due to be reviewed annually by the CNEA Delivery Group.

### **Legislation**

6. The Data Protection Act 1998, in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data) in most formats – e.g. paper, electronic, images (photographic/video), etc.
7. The key legislation governing the collection and use of personal information include:-
  - The Data Protection Act 1998
  - The Human Rights Act 2000
  - The Crime and Disorder Act 1998
  - Common Law Duty of Confidentiality
8. The principle elements of the legislation and notes on interpretation of key factors are provided in Appendix B.

9. In respect of the CNEA, information may be shared between MKC, TVP and Parish Council Officers as long as they have signed up to the protocol.

10. The following legislation will also be relevant to us.

- Clean Neighbourhood and Environment Act 2005
- Environmental Protection Act 1990
- Police Reform Act 2002
- Anti Social Behaviour bill 2003
- The Freedom of Information Act 2005

### **Withdrawal from Protocol**

11. 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.

### **“Golden Rules”**

12. As parties signed up to this Protocol, we recognise the importance of sharing information with each other, in line with the aims of the Crime and Disorder Act 1998 and the CNEA 2005, for the purpose of reducing and detecting crimes.

13. 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 Crime and Disorder Act 1998, and in accordance with the Home Office guidance associated with these Acts.

14. We pledge to consult with each other through the CNEA Delivery Group on matters of policy and procedures, and annually with each other upon matters contained within the CNEA Protocol.

15. We undertake in this Information Exchange Protocol that, where possible and appropriate, information requested in the correct manner (see Process section), is given within a time limit of 10 working days; this may vary depending on the nature, volume of requests and operational need.

16. Each partner pledges that all Personal Information remains the property of the disclosing agency, and is the responsibility of the Data Controller as defined by the Data Protection Act 1998. The partner receiving the data will not normally use it for any purpose other than that set-out in this Protocol, nor share it with any other party, without the disclosing partner's written permission.

17. 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.
18. We agree to disclose information to those Agencies who have signed this protocol, so long as the request falls within the framework of this protocol.
19. Further disclosure of the same data to persons/agencies outside this Protocol would be regarded as “Secondary Disclosure” and would not normally be allowed, unless that body was brought into this information-sharing Protocol, in the proper manner
20. Information disclosures are defined further below.
21. Each party to this protocol pledges to check its data notification to ensure that it is appropriately registered for sharing and receiving personal information for the purpose of crime reduction. Each party also pledges to ensure that the data it holds is as accurate and up to date as possible.
22. We agree when handling the Media,
  - To be fair to our fellow partners, and maintain their integrity
  - When providing information to the public, to do so honestly and fairly
  - Statements must reflect the multi-agency decision process
  - Consent of the data owner will be sought prior to release to the media
  - Where personalised information (relating to individuals) is already in the public domain, express permission from the subject must be obtained before any response is given.

## **Non-personal Information**

23. We understand that non-personal information constitutes data that has never referred to individuals. Non-personal information is more often than not aggregate data. [see Appendix A - Glossary]. It is non-personal information (never has referred to an individual) or aggregated data (derived from personal, non-personal and de-personal information), that is normally used for crime-mapping. We can use this non-personal information for crime-mapping purposes, within the remit of the Crime & Disorder Act 1998 and the CNEA 2005.
24. We agree that non-personal information held by us may be subject to the provisions of the Freedom of Information Act 2000. We have the legal duty to provide non-personal information to a third party, if a formal request is made.

25. We will disclose non-personal information for the purpose of profiling local areas for crime activity.

## **Depersonalised information**

26. We understand that depersonalised information 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 Commission 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.

27. We accept there are no legal restrictions on the exchange within this Protocol of depersonalised information, 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.

28. We appreciate that if several sets of depersonalised information were merged or compared to each other, there is a risk that an individual could be identified. We will always hold depersonalised information securely and destroy it securely, when no longer required.

## **Personal information**

29. We understand that personal information is information which relates to a living individual who can be identified from the data; this data will be clearly marked as personal information 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 information when no longer required for the purpose for which it was provided.

30. We undertake to formally record all grounds for disclosure of personal information. We will process information 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.

31. Personal information 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 (See Appendix B)
- b) The proposed disclosure of personal information 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.

32. Section 115 of the Crime and Disorder Act 1998 provides us with lawful power for disclosure where this is for the purpose of implementing the provisions of the Crime and Disorder Act. However, although the Act creates a situation where the disclosure of information may be lawful, the presumption of confidentiality will still apply.
33. Apart from the exceptions stipulated in this section, we will only disclose Personal information relating to any individual with the express consent of the data subject. This will be to designated staff or posts to enable them to carry out their duties in the exercise of a public function as stipulated in this protocol.
34. We can also disclose on a case-by-case basis without the consent of the data subject, 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):
- To prevent or detect crime
  - To apprehend or prosecute offenders
  - If it is required by law (bulk disclosures are also normally allowed)
  - If the disclosure is registered with the Information Commissioner.
35. When information is disclosed under this section, the data subject must be informed. When disclosure is required, we agree to ensure that;
- The information is being processed lawfully and fairly
  - The public interest is of sufficient weight to override 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
  - A disclosure is necessary to support action under the Crime and Disorder Act
  - Any disclosure must have regard to specific statutory restrictions on disclosure.
36. We understand the Public Interest criteria, to include;
- The administration of justice
  - Maintaining public safety
  - The apprehension of offenders
  - The prevention of crime and disorder
  - The detection of crime
  - The protection of vulnerable members of the community.

## **Non – disclosure exemptions**

37. We agree any request for information by a partner must specify as clearly as possible, how failure to disclose the information would jeopardise the objective, as set-out in s29(3) of the Data Protection Act 1998. It must be stated why the case might fail without this information, and what the assumed effect of the successful case might be, following successful disclosure.

## **Human Rights Act 1998**

38. 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;

- National Security
- Public Safety
- Economic well being of the country
- The prevention of crime and disorder
- The protection of health or morals
- The protection of the rights or freedoms of others.

## **Confidentiality**

39. We undertake that information will only be used for the purpose for which it was requested, and will securely store it and destroy it when no longer required. We understand that outside agencies wishing to be part of the information sharing process, will upon signing this protocol, be bound to comply with its terms.

## **Youth Offending teams**

40. It is permissible for information to be disclosed to the members of a youth offending team (or local youth justice team) for the purpose of any provision of the CNEA 2005.

41. Following the initial referral, designated officers attached to the team will be responsible for the further disclosure of relevant personal information and conviction data.

42. There may be occasions when it is necessary for members of the youth offending team to disclose personal information to another agency. In such circumstances the following guidelines must be followed:

- A secondary disclosure of personal information must generally be authorised by the original data owner.

- The disclosure must support action under the CNEA 2005
- The public interest must outweigh any duty of confidentiality and must justify any interference with the right to privacy under Article 8 of the European Convention of Human Rights 1998.
- The information must be processed fairly.

43. The youth offending team manager will be responsible for ensuring that personal information provided to the team is stored in a secure place and destroyed when it is no longer required.

## **Transfer of information**

44. Personalised information should be transferred only by secure methods that are mutually agreed between the relative Principal Designated Officers and Designated Officers.

## **Designated Officers**

45. We understand that each partner must appoint a Primary Designated Officer (PDO see glossary), who will have a co-ordinating and authorising role. We may also appoint further Designated Officers (DOs) within the same body. These individuals are designated to assume responsibility for data protection (including notification where appropriate), security and confidentiality, and compliance with all relevant legislation.

46. Our specific responsibilities will be the following;

- Making sure the parties abide by the sections of this Protocol.
- Ensuring that all DOs and other staff are fully aware of their responsibilities.
- Appointing other staff in the body to act as DOs in their absence.
- Authorising the body's involvement and co-operation in the information sharing process, at every stage.
- Keeping a Protocol Co-ordination Folder, which holds all the partner's information sharing documents in general. This folder or file will be managed by us, PDO or DOs, to ensure that it is accurate and up to date. We must ensure that the information held is reviewed with our partners by arrangement but at least quarterly.
- Ensuring the body's Data Protection Notification entry is accurate, up to date and adequate for the purpose for which it is intended.
- The folder or file must include; a) Record of data disclosed b) Project chronology c) Project access list d) Notes of meetings with our partners, and recent correspondence and phone calls.
- The PDO is the data owner. As such, any final decision on whether to share sensitive information rests with us.

47. Only DOs and PDOs of each body can make the formal requests and document agreements for the sharing of personal information. We can decide (on a case by case basis,) why a disclosure is necessary to support action under the CNEA 2005. We will also decide why and when the public interest overrides the presumption of confidentiality.
48. It is our responsibility to ensure that processing of the Personal information held, is in keeping with the principles of the Data Protection Act 1998, namely;
- It is obtained, processed and disclosed fairly and lawfully.
  - Kept securely.
  - Processed in accordance with the rights of the data subjects.
  - Accurate, relevant and held no longer than necessary.
  - Disclosed only for a specified related purpose.
  - Disclosed without the subject's knowledge and/or agreement only where failure to do so would prejudice the objective.

## **Process**

49. Agreed disclosure procedures will generally require making a request in writing. The reply to this request will normally be made within 10 days. As part of the reply the disclosing party will give an estimate of how much time is required for fulfilment and delivery.
50. Access to personal information by staff other than the Designated Officer, should be limited to employees whose work is directly related to the project and those working within the enforcement role of the CNEA 2005, provided they are signed up to the protocol.
51. 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, we 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.
52. We must agree the criteria for the review and weeding of data in accordance with existing policies and codes of practice. This should cover variations of data held by us and we should agree a maximum retention period for each item of data as stipulated below.

## **Security & Data Management**

53. 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.
54. We agree to the following in respect of personal information:

- When stored on a computer system, it must be password protected and we agree this password will be revised regularly.
- When manual, be stored in a secure filing cabinet when not in use.
- Be located in a secure environment.
- Not be inputted/accessed without industry standard security devices as defined by BS7666.

55. **The national standard for making data “fit for use” is industry standard BS 7666.** This is the standard for describing the location of types such as addresses, rights of way and streets. As most public sector data has a location element to it, this is a good standard to convert disparate data sets from different systems and agencies and fully integrate them. We agree that in order to “future proof” this Protocol, we undertake to use industry standard BS7666 to process our data.

56. All data, including personal information, held by us is subject to a specified “shelf-life” as agreed upon receipt.

57. We understand that all these measures need to be taken to ensure the security of our partners and to protect the general public.

58. We are aware that only the minimum amount of information should be disclosed, in order to get the job done and for the purpose for which it was intended. We agree that all information retained by us and our partners should be kept securely and for not longer than is strictly necessary.

## **Complaints And Breaches**

### **Complaints:**

59. Initial complaints must be referred to the appropriate PDO or DO and we agree in this Protocol, the procedure to be followed in the event of such a complaint being received, is to refer the matter to the individual organisation’s complaints procedure.

60. 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.

61. We undertake to do all that we can within the guidelines of the Data Protection Act 1998, to assist with any complaint.

62. Individuals do retain the right to raise a complaint with such bodies as the Information Commissioner or the statutory Ombudsman.

## **Breaches:**

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

## **Audit**

65. **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.
66. **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. It is the responsibility of each Partner to ensure that their security arrangements are adequate and fit for purpose.
67. **Audit of Protocol:** We undertake to conduct an annual audit of this Protocol, in order to amend it and ensure it remains fully effective.

## **Signatories**

68. This Protocol must be signed by a representative of sufficient standing from each of the named parties. The signatories to the Protocol recognise and accept the principles laid down in this document as a legal and secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional obligations and responsibilities

## Appendix A - Glossary To The Protocol

<b>AGGREGATE DATA:</b>	Data that consists of statistics of events forming a trend or pattern but from which it is not possible to identify individuals.
<b>AUDIT TRAIL:</b>	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.
<b>CLEAN NEIGHBOURHOODS AND ENVIRONMENT ACT 2005:</b>	The Purpose of this act is increase powers to deal with offences regarding Quality of Life issues. It is, also, the act that provides Parish Councils with powers to deal with litter, graffiti, fly posting and nuisance involving dogs.
<b>COMMON LAW:</b>	The principle underlying all criminal-related work is the common law duty of confidentiality 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.
<b>CRIME:</b>	Any act, default, or conduct prejudicial to the community, the commission of which by law, renders the person responsible liable to punishment by fine, imprisonment or other penalty.
<b>CRIME AND DISORDER ACT 1998:</b>	The purpose of the Act is to tackle crime and disorder and help create safer communities
<b>CRIME AUDIT:</b>	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 anti-social behaviour.
<b>CRIME MAPPING:</b>	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.
<b>DATA:</b>	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.
<b>DATA IN THE PUBLIC DOMAIN:</b>	Any information which is publicly available, whether it relates to a living individual or not. For example, Information found on the internet, television or local authority records.
<b>DATA OWNER:</b>	This is the individual or partner who is responsible for complying with the eight Data Protection

principles, as set-out in the Data Protection Act 1998. It is the owner's responsibility to ensure that the data is securely stored.

- DATA PROCESSING:** This term is used to describe the collecting, handling, sanitising, transferring and storing of all types of data.
- 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 information, 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.
- DISORDER:** Refers to the level or pattern of anti-social behaviour within a certain area.
- FORMAL REQUEST:** A written request by the Designated Officer for personal information made to the information holder.
- HUMAN RIGHTS ACT 1998:** This Act requires the compliance to Article 8 of the European Convention on Human Rights. This allows interference with the right to respect for private and family life only when it is in accordance with the law, and pursues a legitimate public interest in a proportionate manner.
- 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 used to inform decision-making.
- NON-PERSONAL INFORMATION:** Any information which does not or cannot be used to establish the identity of a living individual.
- PERFORMANCE INDICATOR:** Tool to measure the success/failure of an objective

**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 holder. This is the most restricted type of information and should only be used where there is no reasonable alternative.

**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.

**REVIEW:**

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

## Appendix B

- 1) **The Clean Neighbourhood and Environment Act 2005** – ensures that local Crime and Disorder Reduction Partnerships will take anti-social behaviour affecting the local environment into account in developing crime and disorder reduction strategies.

Powers that can be taken up by Parish Councils are as follows:-

<p>To make dog control orders.</p>	<p>The Act gives parish councils the power to make dog control orders. A parish council can make and apply dog control orders, to cover land in its area, making it an offence to:</p> <ul style="list-style-type: none"> <li>• Fail to remove dog faeces;</li> <li>• Not keep a dog on a lead;</li> <li>• Not put, and keep, a dog on a lead when directed (told) to do so by an authorised officer;</li> <li>• Permit a dog to enter land from which dogs are excluded (banned); and</li> <li>• Take more than the specified (allowed) number of dogs (which a person may take) onto land.</li> </ul>
<p>To take enforcement action against those that:</p>	<p>The Act allows parish councils to prosecute, in the magistrates' court, those that are suspected of committing an offence against a dog control order, or who are suspected of having committed a litter, graffiti or flyposting offence.</p> <p>As an alternative to prosecution in the magistrates' court, the Act gives the power to parish councils to authorise staff to issue fixed penalty notices to alleged offenders as an alternative to prosecution.</p>

[Defra, UK - Environmental Protection - Local Environmental Quality - Clean Neighbourhoods and Environment Bill](#)

- 2) **The Human Rights Act 1998, Article 8** – “Everyone has the right to respect for his private and family life, his home and his

correspondence.” There are specific grounds upon which it may be legitimate for authorities to infringe or limit those rights. The second part of this article states “there shall be no interference by a public authority with the exercise of this right except as 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.”  
<http://www.humanrights.gov.uk>

- 3) **The Data Protection Act 1998** - The key principles of the Data Protection Act are:-
- a) Personal Data must be processed (e.g. collected, held, disclosed) fairly and lawfully and that processing must satisfy one of the conditions in Schedule 2 of the Act. The processing of sensitive data is further protected in that processing must also satisfy at least one of the conditions of Schedule 3 of the Act.
  - b) Personal Data shall be obtained and processed for only one or more specific and lawful purpose(s).
  - c) Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s).
  - d) Personal Data shall be accurate and kept up to date.
  - e) Personal Data shall not be held for longer than is necessary.
  - f) Processing of Personal Data must be in accordance with the rights of the individual.
  - g) Appropriate technical and organisational measures should protect Personal Data.
  - h) Personal Data should not be transferred outside the European Union unless the recipient provides adequate protection.

**Schedule 2** of the Data Protection Act 1998 specifies conditions Relevant to the Processing of Personal or Sensitive Data

- a) The data subject has given his/her consent to the processing
- b) The processing is necessary for:  
the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract.
- c) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract
- d) The processing is necessary to protect the vital interests of the data subject.
- e) The processing is necessary for the administration of justice for the exercise of any functions conferred on any person by or under any enactment for the exercise of any functions of the Crown, a Minister of the Crown or a government

- department for the exercise of any other functions of a public nature exercised in the public interest by any person
- f) The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except when the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

**Schedule 3** of the Data Protection Act 1998 specifies additional conditions relevant for the processing of sensitive personal data, namely:-

- a) The data subject has given his/her consent
- b) Processing of sensitive personal data is necessary:-
- By right or obligation under law
  - To protect specific vital interests of the individual or other persons, where consent cannot be given by or on behalf of the individual
  - In the course of legitimate activities of specified non-profit organisations, with extra safeguards
  - Information already publicly released by the individual
  - Legal, judicial, government or crown reasons
  - Medical purposes
  - To monitor equality or opportunity
  - By order of the Secretary of State.

<http://www.dataprotection.gov.uk>

- 4) **The Crime and Disorder Act 1998** - introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.

Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Act.

Whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the information. It should be noted, however, that this does not exempt the provider from the requirements of the second Data Protection principle <http://www.crimereduction.gov.uk/cdact1.htm>

- 5) **The Freedom of Information Act 2000** - The Data Protection Act, 1998, gives individuals the right of access to personal information held about them. The Freedom of Information Act extends this right of

access to include 'non personal' information. This may include information about a third party. The two laws come together at the point where personal information is considered for disclosure.

Requests for information made by individuals about themselves will be exempt under the Freedom of Information Act, and will continue to be handled as Subject Access Requests under the Data Protection Act.

Where an individual specifically requests information about a third party, or where responding to a request would involve the disclosure of personal information about a third party, the request falls within the remit of the Freedom of Information Act (although Data Protection Principles must still be applied). An authority must not release information about a third party, if doing so would breach one of the Principles.

## Exemptions

There are a number of exemptions to the general right of access contained in the Act. These are listed below:

- information accessible to the applicant by other means (Section 21)
- information intended for future publication (Section 22)
- information supplied by or relating to bodies dealing with security matters (Section 23)
- national security (Section 24)
- information likely to prejudice national defence or the armed forces (Section 26)
- information likely to prejudice the UK's international relations or interests (Section 27)
- information likely to prejudice relations within the United Kingdom (Section 28)
- information likely to prejudice the economic interests of the UK or part of the UK (Section 29)
- investigations and proceedings conducted by public authorities (Section 30)
- law enforcement (Section 31)
- court records (Section 32)
- information held by public authorities which have functions relating to audit (Section 33)
- parliamentary privilege (Section 34)
- formulation of government policy (Section 35)
- prejudice to the effective conduct of public affairs (Section 36)
- information that relates to communications with Her Majesty, a member of the Royal Family or Royal Household, or to the conferring of honours (Section 37)
- health and safety (Section 38)
- environmental information (Section 39)

- personal information (Section 40)
- information provided in confidence (Section 41)
- legal professional privilege (Section 42)
- commercial interests (Section 43)
- legal prohibitions on disclosure (Section 44)

## Amendments to the Data Protection Act 1998

Currently under the Data Protection Act 1998, manual data is considered to be data under the Act only where it forms part of a “relevant filing system” (i.e. where the manual data forms part of a set and is structured in such a way that specific information relating to a particular individual is readily accessible). This definition of data is extended under the Freedom of Information Act 2000 to include manual records held by public authorities (or by other parties on behalf of public authorities), which do not fall within the definition of a “relevant filing system”. This unstructured manual data will be considered to be personal data where it can lead to a living individual being identified.

Section 40 of the Freedom of Information Act 2000 states that information is exempt from disclosure:

- a) where the applicant is the subject of the data. Such requests will be treated as Subject Access Requests under the Data Protection Act;
  - b) where the applicant is not the subject of the personal data but where disclosure of this third party data would breach any of the eight Data Protection Principles; or
  - c) where the applicant is not the subject of the personal data but where disclosure of this third party data would be exempted under the Data Protection Act 1998 (i.e. where the data subject themselves would not be entitled to see this data under the Data Protection Act).
- 6) **Common Law Duty of Confidentiality** - All staff working in both the public and private sectors should be aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this. *‘In confidence’...Information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular where a professional relationship may exist e.g. doctor/patient, social worker/client, lawyer/client etc.*

The duty of confidence only applies to person identifiable information and not to aggregate data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.

The duty of confidence requires that unless there is a statutory requirement or other legal reason to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm).

Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, the Department of Health and relevant professional bodies accept that there is an ethical duty to respect the confidentiality of the dead.

Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained before disclosure of their information.

Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence. Where it is judged that an individual is unable to provide informed consent (due to age or condition), schedule 2 and 3 of the Data Protection Act 1998 must be satisfied (processing will normally need to be in the vital interest of the individual). 'Public functions' as outlined in schedule 2 and 'medical purposes' as outlined in schedule 3 of the Data Protection Act 1998 are also likely to be relevant.