

<b>Recording of Clients of Concern Policy and Procedure</b>	Reference: *
	Version No: *.*
	Issue Date: *
	Classification: *

### Document Control

<b>Document Ref:</b>		<b>Date Created:</b>	Dec 2009
<b>Version:</b>	1.0	<b>Date Modified:</b>	
<b>Revision due</b>	Dec 2012		
<b>Author:</b>	Ian Priestley	<b>Sign &amp; Date:</b>	
<b>Head of Service:</b>	Andy Walker	<b>Sign &amp; Date:</b>	
<b>Equality Impact Assessment: (EIA)</b>	Date undertaken:		
	Issues (if any):		

### Change History

Version	Date	Description	Change ID
0.1			

### Related Documents

Reference	Title	Tier
	Protection of Staff Policy	
	Procedure and Guidance on Managing Violence and Aggression against Staff	
	Policy and Procedure for the Recording of Clients of Concern	

# Contents

---

1.	Policy.....	3
1.	Applicability .....	3
2.	Roles and Responsibilities .....	3

## **Procedure**

3.	Responsibility for the management of the Clients of Concern database .....	4
4.	The Role of Gatekeepers.....	4
5.	Including a record onto the Clients of Concern Database .....	5
6.	Undertaking a Review of Records on the Clients of Concern Database .....	6
7.	Data Protection .....	7
8.	Access to records.....	7

DRAFT

## **1. Policy**

- 1.1. West Berkshire Council is committed to minimising the risk of assault to employees operating away from Council Offices.
- 1.2. In order to balance the requirements of the Council to protect employees with the legitimate rights of the public, the policy of West Berkshire Council is to undertake record-keeping measures to ensure staff are aware of those persons who are known to pose or suspected of posing a risk to the safety of employees.
- 1.3. Records of such individuals will be maintained on a register (known as the 'Clients of Concern' register).
- 1.4. The Council recognises that personal data processed within the records of people likely to pose a risk to staff constitutes 'sensitive' personal data, as defined in section 2 of the Data Protection Act 1998. The procedure that accompanies this policy has been written to ensure collation and storage of the data is controlled and complies with the requirements of the Act.
- 1.5. The measures outlined in this policy and procedure form part of a wider remit to maintain the Health and Safety of WBC employees and should be used in conjunction with the Protection of Staff policy, the Procedure and Guidance for Managing Violence and Aggression against Staff and Guidance for service areas on the development of service-specific Lone Working procedures.
- 1.6. The Chief Executive and Corporate Board have approved the Recording of Clients of Concern Policy and Procedure.

## **1. Applicability**

- 1.1. This Policy applies to:
  - 1.1.1. All non-school based employees working for the Council, including those working from home or at non-Council locations.
  - 1.1.2. Other persons including Elected Members, consultants, agency staff and contractors working for the Council, external organisations working with the Council, whilst engaged on Council business .
- 1.2. This Policy has been the subject of consultation with Heads of Service and trade unions and has been ratified by the Council's Corporate Board.

## **Roles and Responsibilities**

- 2.1. Heads of Service have overall responsibility for ensuring the recording of clients of concern is managed appropriately in accordance with this agreed procedure within their service areas. The specific responsibilities of Heads of Service are detailed in the relevant sections of the procedure.

- 2.2. The Health and Safety Team are responsible for maintaining this policy and procedure and for providing advice and guidance on implementation. The Risk and Safety Manager also has a key role in the management of the Clients of Concern database (see section 3).
- 2.3. It is the responsibility of each employee and other person mentioned in Section 2.1. to familiarise themselves with and adhere to this policy and procedure.
- 2.4. In particular, where an employee, or other person included in 2.1 of this policy/procedure, becomes aware of a client of the Council whose behaviour, either actual or threatened, poses a risk to the health or safety of Council employees, he/she must report the details of the incident to his/her line manager or other senior officer in the relevant service area.
- 2.5. In addition, employees who, given the nature of their statutory responsibilities, may expect to experience conflict with clients during the course of their duties, will be given access rights to the Clients of Concern Register and must check the register prior to making a visit to a client's premises.
- 2.6. All employees who have access to the Clients of Concern Register have specific responsibilities under the Data Protection Act and must ensure compliance at all times.
- 2.7. In addition, 'Gatekeepers' have specific responsibilities with regard to the Clients of Concern Register (see section 4 for more detail on the role of Gatekeepers).

### **Responsibility for the Management of the Clients of Concern Register**

- 3.1. The purpose of the Clients of Concern Register is to record details of clients who are known to pose, or who are suspected of posing, a threat to the safety of West Berkshire Council employees. The Register can be used as a measure to protect the safety of employees who are required to visit clients away from Council offices.
- 3.2. Management of the Clients of Concern Register is the responsibility of the Clients of Concern Group.
- 3.3. This Group comprises nominated 'Gatekeepers', who represent relevant service areas, and the Health and Safety Manager.
- 3.4. Any changes to the management of the Register must be approved by the Clients of Concern Group.

### **The Role of Gatekeepers**

- 4.1. Gatekeepers within each relevant service area are responsible for the maintenance and operation of the Register within their service area. The Gatekeeper will create, edit, delete and view records of individuals held on the Register.
- 4.2. Due to the nature of the role, the gatekeeper must understand the sensitive nature of the records and the need to comply with the Data Protection Principles (see Section 7 below).
- 4.3. The gatekeepers must also understand that the implications of any failure to accurately record details of any persons likely to pose a risk to staff are very

serious for both individual employees and the Council as a whole. Failure of a gatekeeper to adhere to this policy and procedure may result in disciplinary action.

- 4.4. Heads of Service nominate gatekeepers for their service areas and ensure this list is maintained. The Head of Service will also notify ICT, who will provide gatekeepers with appropriate access rights to the database.
- 4.5. The Head of Service must also ensure the gatekeepers are aware of, and comply with, the Data Protection Principles in section 7.
- 4.6. A gatekeeper must ensure reasons for the inclusion of an individual on the Clients of Concern Register are maintained (see 5.7) and, where required, must be prepared to justify to the Clients of Concern Group, or the Information Commissioner, why a record has been maintained.
- 4.7. A gatekeeper is also responsible for maintaining the accuracy of each record he/she inputs onto the register and is also responsible for reviewing the continuing retention of each record (see Section 6 - Undertaking a Review).

### **Including a record onto the Clients of Concern Database**

- 5.1. Gatekeepers within each relevant service area are responsible for inputting records of individuals onto the database.
- 5.2. Where an employee, or other person included in 2.1 of this policy/procedure, becomes aware of a client of the Council whose behaviour, either actual or threatened, poses a risk to the health or safety of Council employees, he/she must report the details of the incident to his/her line manager or other senior officer in the relevant service area.
- 5.3. Examples of such behaviour could include, but not be limited to:
  - Threats of violence
  - Physical assault
  - Sexual assault
  - Verbal abuse
- 5.4. The line manager/appropriate senior officer should record the incident, using their service areas' normal method of record keeping but then, in consultation with the head of service, instruct the gatekeeper to make an entry onto the Clients of Concern Register, selecting one of the 'drop down' classification of risk available (Physical, Verbal, Sexual, Other).
- 5.5. Where a record of the individual is to be maintained on the Clients of Concern Register, the Gatekeeper should record the following details within their own record keeping system:
  - The name of the person posing the risk
  - The address at which they reside

- The classification of the risk posed.
- The degree of risk posed to council officers and why.
- The name of the Head of Service making the decision to record
- The date on which the record was made
- *Note – section 8.6 also refers to an Owner of the record – not sure who this is and how they would fit into the process to determine who should be included on the database – could this be clarified?*

5.6 Each time a new entry is made into the register by a gatekeeper, he/she shall alert other service's gatekeepers to the new entry by emailing the Gatekeeper distribution group

### **Undertaking a Review of Records on the Clients of Concern Database**

6.1. A gatekeeper is responsible for reviewing each record he/she inputs onto the Clients of Concern Register. Heads of Service are responsible for ensuring this happens.

6.2. Review intervals for each record held on the database should not exceed 6 months. Factors a gatekeeper, in consultation with a senior officers currently dealing with that client, should take into account when determining whether a record should continue to be retained include:

- An assessment of the level of violence of the incident which led to a record being made
- The gravity of the incident
- The length of time that has elapsed since the original incident
- The previous and subsequent behaviour of the individual
- Whether the incident was likely to have been a 'one-off'
- Whether it is likely that the individual will become violent again
- Any changes in the condition of the premises where the incident occurred
- The continues presence of dangerous animals at the premises, where applicable
- Changes of address

6.3. The gatekeeper should ensure the date of the review and the outcome are recorded on the Register.

## **7. Data Protection**

7.1. The items recorded on the Clients of Concern register constitute 'sensitive personal data' as defined in section 1(1) and section 2 of the Data Protection Act 1998 (the Act).

7.2. Gatekeepers will ensure they comply with the following eight data protection principles:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose/those purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7.3. The gatekeepers should attend the 'Using Information at West Berkshire Council' training course to obtain further training on the Data Protection Act and the management of data.

## **8. Access to records – Authorised Users**

8.1. Access to records held on the Clients of Concern Register will only be available to staff who have a legitimate reason to access the information – i.e. the personal safety of those staff would be endangered if access to the Register was not granted.

8.2. Such staff are likely to be employees who, given the nature of their statutory responsibilities, may expect to experience conflict with clients during the course of their duties, due to having to visit clients in their own homes or upon their own business premises.

8.3. Access rights to the Register are determined by the relevant Head of Service who will notify ICT to provide the appropriate access for the designated employees. The Head of Service will ensure any changes to employee status are notified to ICT

immediately (e.g. where an employee moves role, to one where access to the database is not required).

- 8.4. The Head of Service must ensure employees with access rights to the Clients of Concern register are made aware of responsibilities under the Data Protection Act, and employees should attend the 'Using Information at West Berkshire Council' training course. In essence, an authorized user of the register must not share the data with any external agency or any other West Berkshire Council employee (or contractor) unless that person has likewise been authorized to use it, given the nature of their job. A list of authorised users are to be held electronically with the register i.e. within the same Excel 'workbook'.
- 8.5. Prior to attendance at a premise, authorised users must check the Clients of Concern Register for the existence of records of a person posing a risk. Where such a record exists, he/she must make contact with the relevant gatekeeper, listed with that record, **before** attempting to visit that client.
- 8.6. Having consulted with the relevant gatekeeper regarding their service team's current estimation of risk involved with visiting that client, the authorised user can then make an informed decision as to whether their personal safety is likely to be compromised by making a lone visit to that client.
- 8.7. Where the authorised user does feel that their Personal Safety may be compromised, he or she should either take a fellow officer or a police officer with them on that home / business premises visit. Alternatively, where possible, the authorised user should require the client to come to an appointment at the council offices, whereby a meeting can be held with two officers, within a suitable meeting room, ideally equipped with a security alarm.
- 8.8. Responsibility for the Clients of Concern Register.
- 8.9. The overall responsibility for the Clients of Concern Register and the system of authorised access to and use of the data will be that of the Risk & Safety Manager.
- 8.10. The Risk and Safety Manager will regularly monitor the content of the register to ensure that review dates are not being exceeded by any particular gatekeeper.
- 8.11. The Risk and Safety Manager will also periodically check that gatekeepers and authorised users are able to easily access the register and make new entries where necessary.
- 8.12. The Risk and Safety Manager will also promote the use of the register for all service areas where staff are required to undertake home or business premises visits to clients, in the interests of their personal safety.