



DATA PROTECTION ACT 1998

GUIDANCE NOTE 11 - THE USE OF RISK MARKERS

**Prepared By: Patricia Rowson
Corporate Information
Governance Officer**

**Date of Publication:
Version: 1.0**

Table of Contents

1. Version Control	3
2. Points of contact for this Guidance	3
3. Introduction	4
4. Compliance with the Act - fairness	4
5. Compliance with the Act - processing conditions	5
6. The individual's rights	5
7. Passing the information to other organisations	6
8. Retention	6
9. Security.....	6
10. Process of assignment.....	7
11. Coding	10
12. Staff training.....	10
13. Advice and Assistance.....	10

1. Version Control

Version	Date	Notes
1.0	15 th September 2010	First draft
1.1	12 th October 2010	Feedback from contacts following initial circulation
1.2	22 nd October 2010	Second draft following review at 14 th October workshop

2. Points of contact for this Guidance

Corporate Information Governance Team

Name	Malkiat Thiarai
Title	Head of Information Governance
Telephone	0121 303 1909
Email	malkiat_thiarai@birmingham.gov.uk

Document Author

Name	Patricia Rowson
Title	Corporate Information Governance Officer
Telephone	0121 303 4876
Email	patricia_rowson@birmingham.gov.uk

3. Introduction

The use of warning markers

This guidance explains to managers of staff working with the public how best to manage the use of warning markers. This guidance covers only the use of 'risk marker' where the threat to an employee's health and safety is posed by an individual. It does not cover other risks, such as risk from a property or location. These risks will be covered by relevant Health and Safety procedures.

Warning markers

Employers have a duty of care to their staff to protect them at work. This will include Council offices as well as other locations where staff may be required to attend as part of their duties.

Health and safety legislation such as the Health and Safety at Work Act 1974, Management of Health and Safety at Work Regulations 1999 and the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 provide the legislative framework to which employers must comply when considering how to protect staff at work. Further information in respect of Health and Safety obligations can be obtained from the Corporate or Directorate Health and Safety teams.

Warning markers are a means of identifying and recording individuals who pose, or could possibly pose, a risk to the members of staff who come into contact with them. It is understood that, in practice, a flagged piece of text is attached to an individual's file. These markers should be used very carefully and should contain the reasons for marking the individuals' record with a warning marker. When making a decision whether a record should be marked the following risk factors should be considered:

- Nature of the incident (physical or non-physical)
- Degree of violence used or threatened by the individual
- Injuries sustained by the victim
- The level of risk of violence the individual poses
- Whether an urgent response is required to alert staff
- Impact on staff
- Impact on provision of services
- Likelihood that the incident will be repeated
- There is likely to be further contact with the individual in the near future
- The incident, while not serious itself, is part of an escalating pattern of behaviour
- Other risks / threats that have the potential to present a risk to the health and well being of staff, carrying out their duties in the normal course of business

4. Compliance with the Act - fairness

The first data protection principle requires that the processing must be fair and lawful. This means that a decision to put a marker on an individual's file must be based on a specific incident or expression of clearly identifiable concern by a professional rather than in response to a general opinion about that individual. The individual should pose a genuine risk and the decision should be based on objective and clearly defined criteria and in line with a clear and established policy and review procedure. The criteria should take into account the need to accurately record any incident.

For consistency, you should make sure a senior nominated person in the organisation is responsible for making these decisions. Decisions should be reviewed regularly. When making a decision this person should take into account:

- the nature of the threat;
- the degree of violence used or threatened; and
- whether or not the incident indicates a credible risk of violence to staff

Records of all decisions should be recorded in order to defend any claim for either defamation, investigation by the Information Commissioner's Office or Local Government Ombudsman or breach of the Data Protection Act.

For the processing to be fair, you should normally inform individuals who have been identified as being a potential risk soon after you make the decision to add a marker to their record. It should be part of your procedure to write to the individual setting out why their behaviour was unacceptable and how this has led to the marker.

You should tell them:

- the nature of the threat or incident that led to the marker;
- that their records will show the marker;
- who you may pass this information to; and
- when you will remove the marker or review the decision to add the marker.

There may be extreme cases where you believe that informing the individual would in itself create a substantial risk of a violent reaction from them, for example, because of the nature of the incident or the risk to another individual. In these cases it may not be sensible to inform the individual as described earlier.

If this is the case, you must be able to show why you believe that by informing the individual of the marker there would be a substantial risk of further threatening behaviour.

You should make all decisions on a case-by-case basis and keep records.

5. Compliance with the Act - processing conditions

The Act states that you should not process personal data unless you can meet one of the conditions in schedule 2 of the Act, and for sensitive personal data, one of the conditions in schedule 3.

As employers have a duty of care towards their staff, for example, under health and safety legislation, the appropriate schedule 2 condition to allow processing of information in markers is that processing is necessary to comply with any legal obligation imposed on the data controller (which in this case would be the employer). The appropriate schedule 3 condition is that processing is necessary to comply with any legal obligation imposed on the data controller in connection with employment.

6. The individual's rights

The Act gives individuals the right to make a subject access request. In most circumstances, you should reveal the fact that there is a warning marker on the individual's record, although, in most cases, you should already have informed the individual. However, you should make this decision on a case-by-case basis and consider any other individuals (third parties) that may be included in the information.

There may be rare cases where you will need to consider whether:

- revealing the existence of the marker;
- revealing the information in the marker; or
- what the individual may infer from the existence of the marker;

May actually cause serious harm to the physical or mental health or condition of that individual. In these cases, you should seek specialist advice from relevant professionals. For some of these cases there may be relevant statutory instruments that modify the provisions in the Act that relate to the individual's rights.

The existence of a warning marker on a person's record should not be used as a basis to refuse to provide services.

Requests from individuals to stop processing their personal information

Section 10 of the Act gives individuals the right to require you to stop processing their personal information if this is likely to cause them substantial and unwarranted damage or distress. If an individual gives you a section 10 notice relating to a violent warning marker then you should be aware that you may ultimately have to justify creating the marker in court.

7. Passing the information to other organisations

From a legal point of view, the appropriate schedule 3 condition for processing mentioned earlier will not cover disclosing the marker information to other organisations, as the condition relates to a legal obligation on the employer for their own staff, not other organisations' staff. However, where there is a good reason for providing the information to another organisation, for example, to alert them to the potential risk to their staff, this will be justified even though no Schedule 3 condition obviously applies. In these cases, our focus is on whether the processing is justified and not unfair.

The senior nominated person in the organisation should determine this on a case-by-case basis where there is a credible risk that an unlawful act, such as an assault, will occur. They should only provide the information to an individual of a similar level in the other organisation.

If you pass the information on to another organisation, you should inform the individual, unless that would be a serious risk to the person or another individual as described earlier. If you review the marker and decide to change or remove it, you should then inform the other organisations you previously sent the information to.

8. Retention

The fifth data protection principle states that personal information should not be kept longer than necessary. You must make sure warning markers / shields are removed when there is no longer relevant to the individual's record. This should be part of the standard review procedure. The retention period is likely to depend in part on:

- the original level or threat of violence, risk or vulnerability;
- the time elapsed since the marker / shield was activated;
- the previous and subsequent behaviour of the individual;
- change in circumstances;
- whether or not an incident was likely to have been a 'one-off';

9. Security

All files containing an indication that an individual presents a risk should be retained securely whether they are paper files or held on computer. You should also take steps to prevent unauthorised access to any information indicating that an individual has had a risk marker flagged against their record.

10. Process of assignment

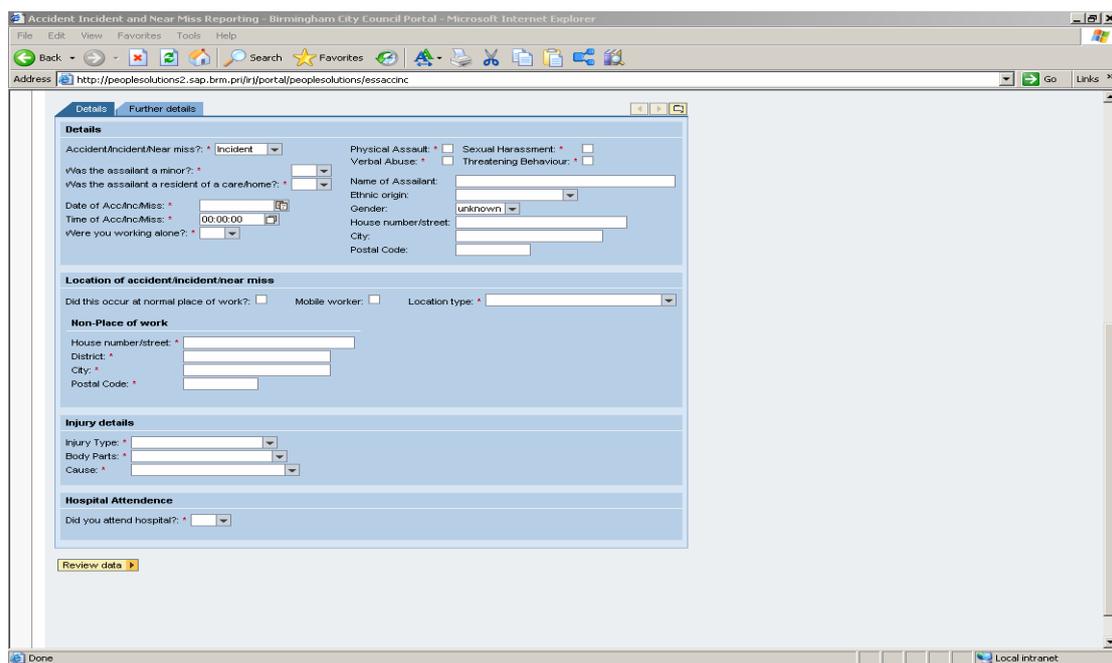
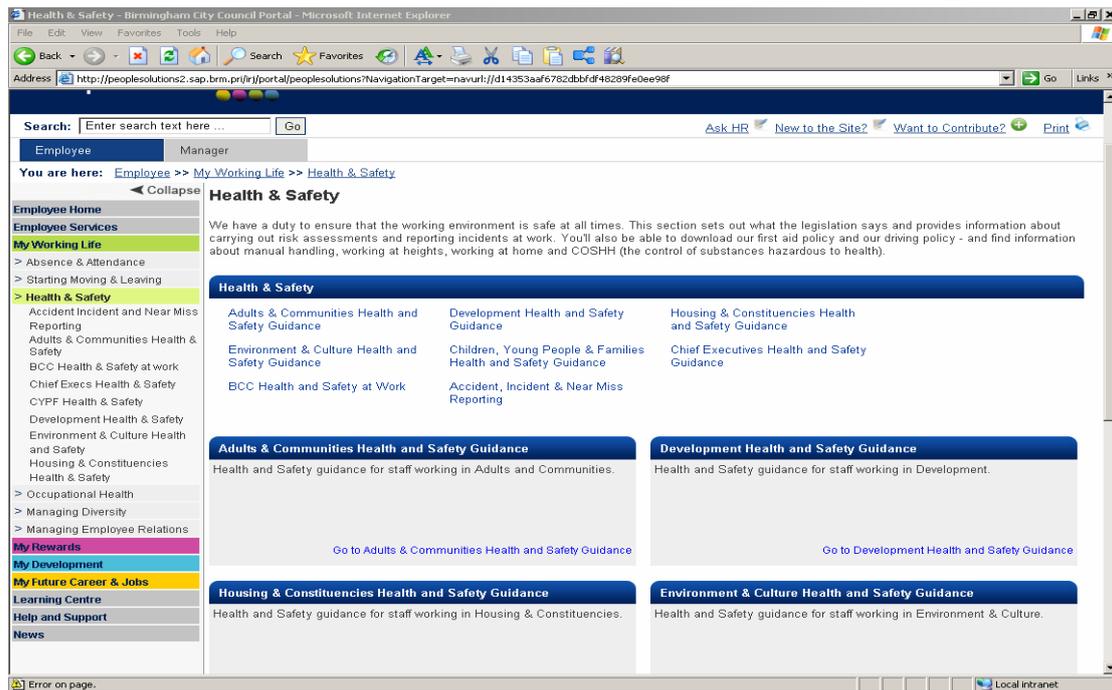
Risk Marker Assignment

The process of a risk marker assignment will involve a two stage process. These are:

- Stage 1: Recording and investigating the incident
- Stage 2: Raising a request for a risk marker to be assigned and shared

Stage 1:

The recording and investigation of the incident should be conducted using People Solutions facility for 'Accident, Incident and Near Miss Reporting' and selecting the 'Incident' reporting process. See below.



The details of the incident should be recorded the employee and submitted to the manager for investigation. Guidance on how to complete these forms is available via People Solutions or via the Health and Safety Teams.

The investigation of the incident should determine, based on an assessment of risk, whether the incident warrants the creation of a risk marker against the individual.

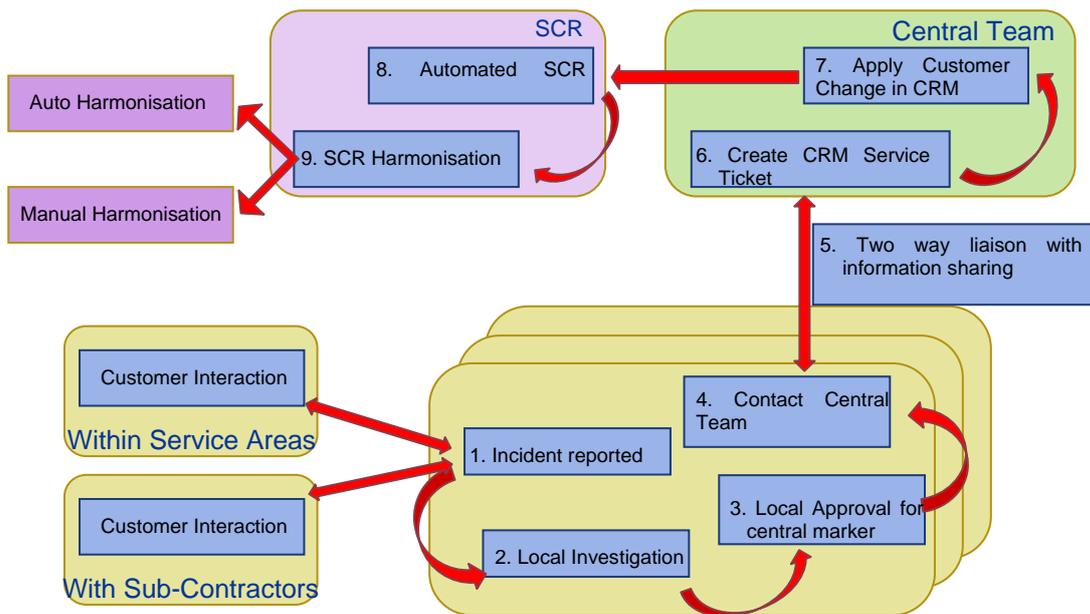
Stage 2:

If, following the investigation, a manager considers that a risk marker should be allocated to an individual then a request should be sent to Customer Services to add a marker to the CRM (Customer Relationship Management) system and the Single Customer Record (SCR). This is likely to involve two way liaison with the Customer Services team to determine whether other flags already exist and what review period is to be set.

The manager is responsible for informing the individual of the Council's intention to place a risk marker against their record.

This information can then be shared across the Council with other services the CRM and SCR.

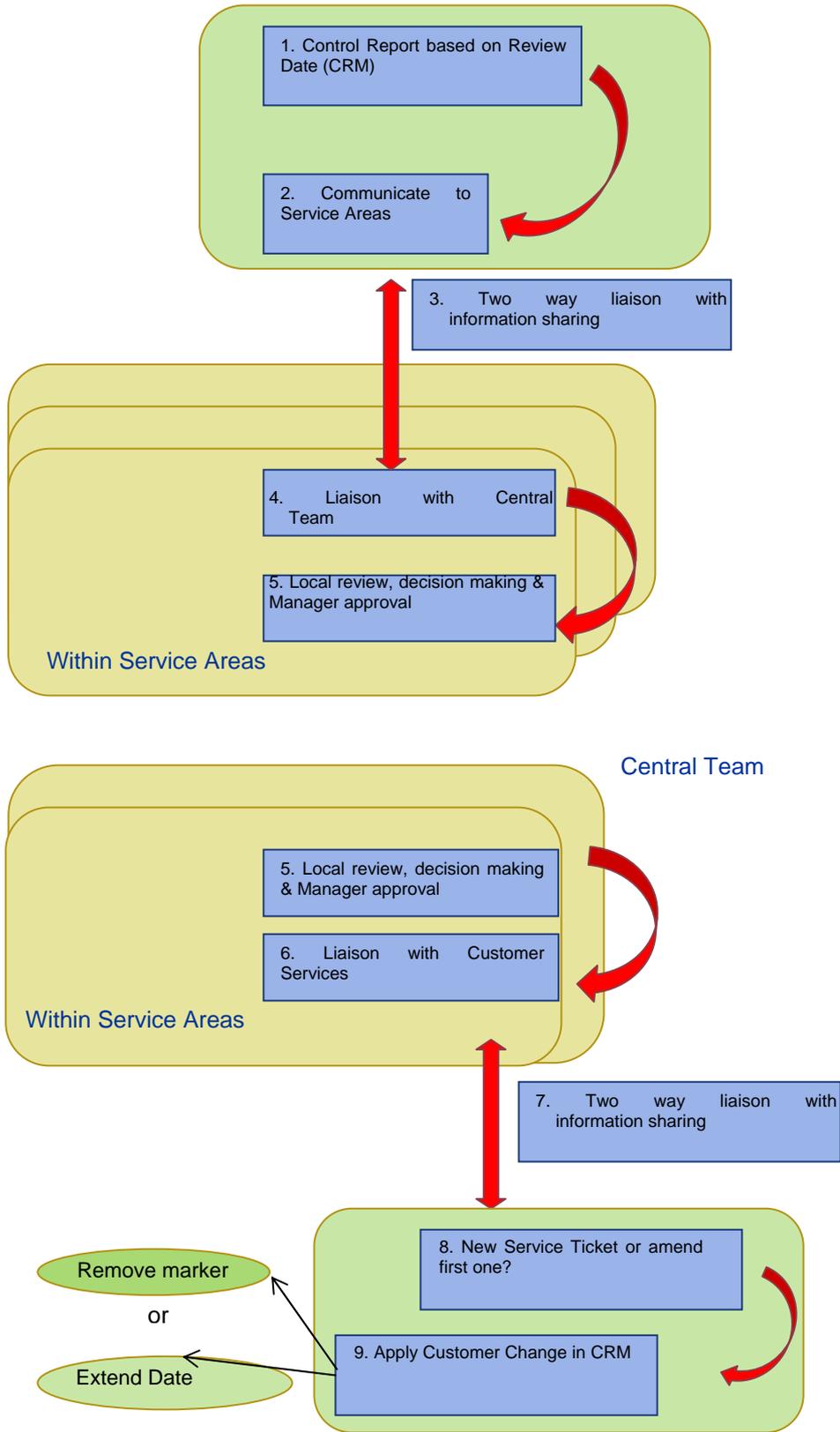
Sharing the Risk Marker information via the SCR



Review process

1. The review process will be triggered based on the review period originally set by the manager when the risk marker was allocated. This should be provided within a specified / agreed period.
2. Set timescales for the review process with an agreed response timescale in order for the risk marker to either be removed or extended, in order to comply with data protection principles.

Central Team



11. Coding

Risk Marker types

Risk Code	Description
100	Level 1 (physical Harm / alleged criminal activity)
101	Physical Assault
102	Legal enforcement
103	Health and Safety at property
104	Risk from animal
105	Risk to under 18's
106	Specific risk to males
107	Possible needle risk
108	Specific risk to females
109	Hate Crime

200	Level 2 (Non physical Harm / standard alert codes)
201	Threatening Behaviour / Verbal Abuse
202	Property Damage
203	Banned from specific council premises
204	Banned from all council premises
205	Banned From Telephone Contact
206	Manager Appointments Only

300	Level 3 Emergency Flag
301	Emergency flag on individual
302	Emergency flag on property / location

12. Staff training

Staff should be trained to use the system and procedures you have relating to violent warning markers. They should be aware of:

- their duty to report all violent or threatening incidents or professional expressions of concern about real or potential violence;
- the process for reporting incidents; and
- the senior responsible person who makes the decisions about markers.

13. Advice and Assistance

13.1 The Corporate Information Governance Team

The Corporate Information Governance Team provides advice and assistance on the Data Protection Act 1998 and the Freedom of Information Act 2000 as well as other associated legislation. The Corporate Team can be contacted on 0121 303 4876 or in writing at the following address:

Corporate Information Governance Team
 Governance Department
 3rd Floor, Lancaster Circus
 1 Lancaster Circus
 Birmingham
 B4 7AB

13.2 Directorate Data Protection Contact Officers

Birmingham City Council has a Data Protection Officer within each individual Directorate in order to provide assistance on data protection issues. If you have any concerns relating specifically to your Directorate please contact your contact officer in the first instance and they will be able to advise you accordingly.

A full list of DP Contact officers is available on In-line.

13.3 The Information Commissioner

The Information Commissioner is the governing body for Data Protection and Freedom of Information and is an independent officer who is appointed by the Queen and reports directly to parliament.

The Information Commissioners duties include:

- Maintaining a register of data controllers
- Distribution of information on legislation
- Promoting compliance with the data protection principles
- Considers complaints about breaches of the principles within the Act
- Prosecutes offenders who contravene the Act

The Commissioner is there to help everyone comply with the Act. If you would like further advice on the Act you can contact the Information Commissioner's office at the address below or you can search their web-site to locate useful information on legislation matters.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545 745