

## Data Protection Good Practice Note

### The use of violent warning markers

This guidance explains to those working with the public how best to manage the use of violent warning markers.

Employers have a duty of care to their staff to protect them in the workplace. Violent 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. We understand 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 identifying individuals as being potentially violent. They are likely to record information relating to:

- the apparent mental stability of an individual; or
- any threatening actions, incidents or behaviour they have or are alleged to have committed.

This means personal data, and often sensitive personal data, will be included in a violent or potentially violent warning marker and so must comply with the Data Protection Act 1998 (the Act).

**INTEC Comment:** InCheck Protector has a full case record to allow all the necessary information to be recorded onto the database, which is then password protected for authorised officers only

This has distinct advantages over simple markers as you can, at any point in time, see clearly why an individual has been given this marker and what the evidence is to back it up. Everything from witness details to images of the injuries/damages caused can be stored on the InCheck System.

InCheck also has the added advantage of being continually supported and developed to meet the ever changing legislative requirements. Most in-house systems take a long time to develop and then have little or no follow up support.

## 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 professional, rather than general opinions 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.

**INTEC Comment:** InCheck protector allows the users to be configured in such a way that only the authorised officer can add new records to the system. INTEC will demonstrate how a 4 tier approach to managing the data is compliant with the Data Protection Act and is also the most efficient way to ensure that regular reviews are carried out on the data held.

The built in reporting tool and reviews manager allows your system administrator (senior nominated person) to carry out regular checks on the data and target those sections where reviews may be due.

For the processing to be fair, you should normally inform individuals who have been identified as being potentially violent 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.

**INTEC Comment:** InCheck protector provides you with the functionality to set up a standard template to be used when notifying every individual and also to note the reasons for not notifying a perpetrator. All of which is recorded on each individual incident record.

**PLEASE NOTE:** It is not acceptable to simply make the decision to never send any letters out as they will all present a risk of further violence. This has to be reviewed on a case by case basis. All this can be recorded and demonstrated with InCheck Protector, should you have any inspections of your compliance with the Act.

## 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.

**INTEC Comment:** InCheck Protector only records information necessary to the incident and protection of staff. Non relevant data (e.g. NINO) is not asked for.

## 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 violent 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. For more information about this, please see our guidance 'Subject access requests involving other people's 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 must get specialist advice from health and data protection 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 (see note 1).

**INTEC Comment:** Once again, InCheck protector provides you with the functionality to set up a standard template to be used for this purpose and also to note the reasons for not notifying a perpetrator. All of which is recorded on each individual incident record.

## 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.

**INTEC Comment:** The 'case management & intelligence database' behind InCheck Protector facilitates this process by giving you ideal functionality to record all necessary information in support of your records.

If the case ever went to court you may have the need to show all evidence from the incident and any related documentation. InCheck will allow you to record all information including

- Witnesses
- Victims
- Pictures of any injuries/damages
- Copies of witness testimonies
- Video clips of the incident in question

## 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.

**INTEC Comment:** Once again, InCheck protector provides you with the functionality to set up a standard template to be used for this purpose and also to note the reasons for not notifying a perpetrator. All of which is recorded on each individual incident record.

## Retention

The fifth data protection principle states that personal information should not be kept longer than necessary. You must make sure violent warning markers are removed when there is no longer a threat. 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;
- how long ago this was;
- the previous and subsequent behaviour of the individual; and
- whether or not an incident was likely to have been a 'one-off'. For example, where the individual was suffering an unusual amount of stress due to a particular set of circumstances.

**INTEC Comment:** All four of the above criteria can be built into the system in conjunction with InCheck's own 'Review Manager' to ensure all data held is reviewed in accordance with legislative requirements.

The 'Review Manager' also provides you with the functionality to provide reports on overdue reviews to the relevant department heads. Reviews can be conducted on the incident record and the people, addresses and vehicle records that may be attached to this case.

The system also has a pre-set 'Skeleton Record' system which allows you to identify and remove unused records in your system, ensuring you are only keeping relevant information.

## Security

All files containing an indication that an individual is potentially violent 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 been violent.

**INTEC Comments:**      **The main InCheck database is password protected and all users can have restrictions on their access to certain parts of the system. 'Subject Access Requests' ensure that every time a user enters a record and audit of when, where from & why they access the information is stored.**

**The search engines will also take a snap shot of the user's details for every search that returns a positive hit. This means that should anyone report suspected misuse of the system you have the reporting/ audit tools to try and identify any suspicious behaviour.**

## 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 name of the person they should report the incidents to; and
- the senior nominated person who makes the decisions about markers.

**INTEC Comments:** Although this is not directly connected to the system this can be added to the implementation costs of our software and training can be given by INTEC. The typical training plan consists of 3 to 4 days training.

**Day One:** This is the system administrator training with guidance and support on how to configure the system accordingly. This will also include time to actually input some of the information.

**Day Two:** This day is normally set up for users of the main database. It will cover every aspect of how to record a case and all associated links (people & Addresses) it will also include search a record to give the relevant feedback

**Day Three/Four:** This day/these days are normally reserved for later in time when the users have more questions and to show the report writing tool. However some customers have used this to training groups of staff on how to use the search engines.

As the search engines are extremely user friendly the majority of users just use handout notes to guide the majority of staff on how to search for a specific record.

**Additional Training can be booked on request.**

## More information

If you need any more information about this or any other aspect of data protection, please contact us.

Phone: 08456 30 60 60 (Lo-call rate)  
01625 54 57 45 (National rate)

Website: [www.ico.gov.uk](http://www.ico.gov.uk)

V2.0  
21.12.06

### INTEC Contact Details:

**T: 0161 976 9633**

**F: 0161 973 6584**

**E: [support@intecpublicsector.com](mailto:support@intecpublicsector.com)**