



# incheckprotector

corporate violent person register

guidance for the implementation  
of a violent person register





**incheckprotector** is the product of INTEC Public Sector. INTEC has worked with local and national organisations for many years, delivering package and bespoke software solutions.



# incheckprotector

## introduction

It is a sad fact that the number violent, aggressive and threatening incidents is on the increase and every organisation now has to take steps to ensure their employees do not see this kind of behaviour as “part of the job” and has to be accepted.

This document will give you the information you need to implement and manage a violent person register. We will use real scenarios taken from our research to illustrate strengths and weaknesses.

## health and safety at work act (1974)

This act states that as an employer you have a duty to identify hazards/risks and introduce necessary controls to ensure, so far as is reasonably practicable, the health, safety and welfare at work of your employees.



## what to look for?

A lot of people ask, ‘what is violent, aggressive and threatening behaviour’? The Health and Safety Executive defines work-related violence as:

*“ Any incident in which a person is abused, threatened or assaulted in circumstances relating to their work ”*

This can include verbal and written abuse or threats, aggressive behaviour or harassment that causes distress (whether in person or over the phone), as well as physical attacks.

However, this does not include anger without being abusive!

## Q. Is your organisation doing enough to protect your staff?



Data Protection Act 1998



Information Commissioner's Office  
Promoting public access to official information  
and protecting your personal information

## legislation

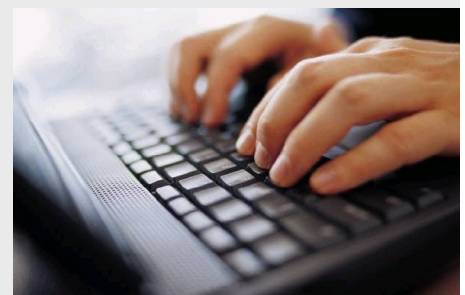
There are numerous guidelines set out by the Information Commissioners Office that need to be adhered to. Failure to meet these guide lines may result in your organisation facing prosecution.

These include the following;

- The 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 .
- A senior nominated person within your organisation should be responsible for making the final decision on whether a person is added to your register. Department heads cannot make this judgement for their individual teams.
- Normally people should be informed that they have been added to such a register. They should be clearly told why they have been added, how long the record will be held and who will have access to this information.
- 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. In these cases it may not be sensible to inform them.

*However, this must be reviewed on a case by case basis. If you decide not to inform the individual, you must be able to show why you believe that informing them would create a substantial risk of further threatening behaviour . It is NOT ACCEPTABLE to simply declare that you will never send out any such letters.*

- You should only process personal data if 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
  - Schedule 2: The processing of information on your markers is necessary to comply with any legal obligation imposed on the data controller (in this case you the employer).
  - Schedule 3: Processing is necessary to comply with any legal obligation imposed on the data controller in connection with employment.
- The Act gives individuals the right to make a subject access request. In most cases you should reveal the fact that they are on your register; though in most cases they would have already been informed. Again, there may be extreme cases where you believe informing the individual would in itself creates a substantial risk of a violent reaction from them. In these cases it may not be sensible to supply this information. This again has to be reviewed on a case by case basis.
- Individuals have the right to use Section 10 of the Act and ask you to stop processing their information. If you are presented with such a request then you may be required to justify creating the marker in court. A spreadsheet will not provide this evidence for you.
- Passing information to other organisations. In general this is not permitted 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 can be justified. In these cases your senior nominated person should make the decision (again, on a case by case basis). The individuals concerned should also be notified of who the information has been sent to.
- These markers should be reviewed on a regular basis and removed (by your senior nominated person) when there is no longer a threat.



If you require more information on these regulations then please contact INTEC.



# incheckprotector

## procedures

Before any form of register can be implemented the organisation has to have a clearly defined set of procedures laid out in the standard employee guidelines. You also need to ensure that staff are fully trained to use these system and procedures.

Specifically, 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.

## suggestions

The common structure for the reporting of these incidents is normally:

1. In the first instance employees should report any incidents to their manager.
2. The line manager should then complete the organisations violent incident report, ensuring as much information as possible is recorded.
3. This form is then sent on to the senior nominated person who makes the final decision on whether to add a marker to the individual's file.

If the individual is added to the register then the Data Protection Act guidelines come into force.

It is also suggested that if an incident report form is declined, the line manager who submitted the report is informed as:


- They have more information on the incident in question.
- It could also highlight the need for more staff training.

## violent incident report form

Your organisation may already have an incident report form. If you do need an example, the form shown below can be downloaded from the HSE Website using the following link:

<http://www.hse.gov.uk/violence/toolkit/reportform.pdf>



 <span style="float: right;">Health and Safety Executive</span>	
<h2>Example violent incident report form</h2>	
Personal details of the person reporting incident	Full name: Job title: Address where incident occurred:
Personal details of injured person	Title: Mr/Mrs/Miss/Ms/Other Name: Home address: Postcode: Daytime telephone: Age: 0-10 <input type="checkbox"/> 11-16 <input type="checkbox"/> 17-25 <input type="checkbox"/> 26-45 <input type="checkbox"/> 46-60 <input type="checkbox"/> 60+ <input type="checkbox"/> Employee <input type="checkbox"/> Customer <input type="checkbox"/> Other (eg contractor, passer-by) <input type="checkbox"/>
Date/Time of incident	Date: _____ Time: _____
Location of incident (including a sketch if possible) and any other relevant information	
Type of incident	Verbal abuse/threat <input type="checkbox"/> Physical attack <input type="checkbox"/> Theft <input type="checkbox"/> Anti-social behaviour <input type="checkbox"/> Near miss <input type="checkbox"/>
Please indicate the nature of the injury you are reporting	Cut <input type="checkbox"/> Burn <input type="checkbox"/> Bruise <input type="checkbox"/> Scald <input type="checkbox"/> Strain <input type="checkbox"/> Other (specify) _____
Please state in detail what happened. Give an account of the incident, including any relevant events leading to the incident and individuals involved including full description of aggressor/assailant(s)	Damage to property:
Who assisted the injured person?	Name: _____
What action has been taken?	Injury related <input type="checkbox"/> Security <input type="checkbox"/> First aid <input type="checkbox"/> Police called <input type="checkbox"/> Ambulance <input type="checkbox"/> Other (specify) _____
Was the injured person taken to hospital and off work for more than 3 days?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Were there any witnesses at the time of the incident?	Name: _____ Contact#: _____ Name: _____ Contact#: _____ Name: _____ Contact#: _____
What action has been taken to ensure that this type of incident does not reoccur, eg have risk assessments been reviewed? Record actions.	
For Management/HR use only:	
RIDDOR Reportable? Yes <input type="checkbox"/> No <input type="checkbox"/> Followed up by Management/HR on (date) _____	



# incheckprotector

## access to the information

The success or failure of a violent person register is based on employees checking and administering the information. Therefore the data has to be made available to anyone who may come into contact with the general public. However, you then have to ensure that employees do not see certain information on individuals that they may never come into contact with.

Organisations tend to combat data security by only giving copies of their database to designated team leaders. The problem with this idea is that it then means your employees have to check with the team leader every time they go out on a visit.

Consider the following scenario;

A man walks into the customer service centre and asks to talk to someone about his property and the neighbour he is having problems with. The receptionist contacts the housing team, the team leader (who has access to the database) is out and one of the female members of the team comes down to see the visitor.

After spending 40 minutes in one of the councils ground floor meeting rooms, the member of staff escorts the man back to reception and returns to her office. At this point her manager has returned and they find that the visitor has an entry in your database that says, "Should not have any one-to-one meetings with female staff members, suspected of assaulting a female visiting officer".

### Q. Could this happen at your organisation?

A. If the officer could check the clients details without having access to the full register, the problem would not have occurred.

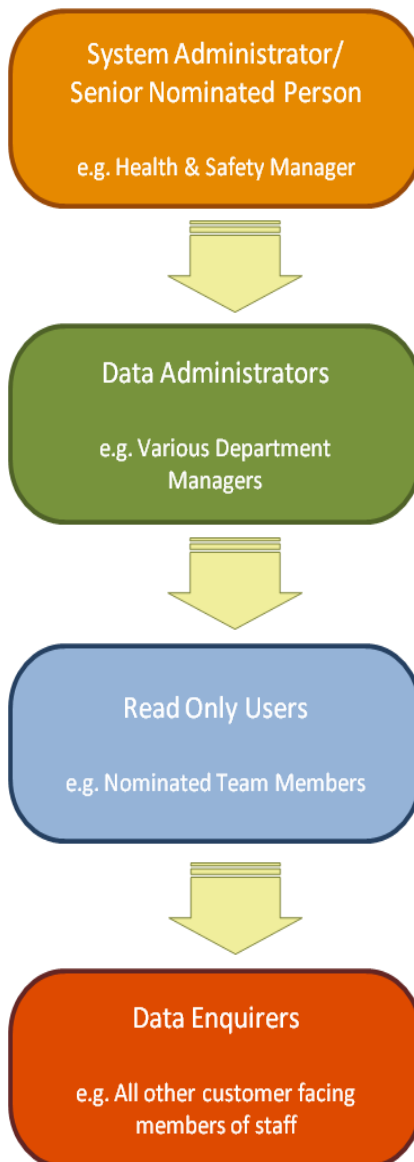
Some organisations we spoke to use very simple lists. In some cases these are just printed off for staff. However, these lists breach various Data Protection regulations so this is not advised. You should have a secure database that prohibits 'browsing' but still has the ability for all staff to check their client's details.

## so what is the answer... incheck

The best way to have your register set up is to allow a selected group of people access to the core database where all information is held, then all other customer facing staff have at least one means of searching the database without seeing the complete list. InCheck Protector gives you this flexibility whilst adhering to Data Protection Guidelines.

This would mean that if your employees were going out to visit a customer, or if a customer came into your offices, they would have a quick and easy way of assessing the risk involved without breaching any of the data protection legislation.

Even those people who do have access to your database should have varying levels of permissions to ensure that your use of information complies with the Data Protection Act. All activity on the database, including any positive searches (i.e. where the searcher has found a match in the database) should be fully audited to deter against data browsing.



## incheckprotector - a four tier approach

The top level user will normally be your senior nominated person. They will have sole control over who is eventually added to, and removed from, your register.

This doesn't mean they will be the only person who can physically add records

Data Administrators will be able to conduct reviews on records and update existing entries to ensure data is correct and up to date.

A working knowledge of the individuals concerned means line managers can review the record better. System Administrators may also carry out additional reviews.

Read-Only users are typically those officers who can log into the database to give, any enquirers more details on potential risks

These users cannot change any data in the system, but by giving various employees this access it means that you have people on site to cover staff working 'out of office'

The vast majority of your customer facing staff will fall into this category. These people will have no direct access to your database, but will be able to your search facilities to check names and addresses

You have to remember that only a very small proportion of the customers you have will appear on these registers.



Other products in our portfolio:

 incaseintelligence

Corporate intelligence solution

 incasebenefits

Benefit fraud case management

 insearchintelligence

Data profiling, mining, analysis and reporting

 informbenefits

Online claims and mobile working solution

 incaseasbo

Anti social behaviour case management

 voicejunction

Automated voice broadcasting and SMS



INTEC Public Sector  
Ashby House  
3 Derbyshire Road South  
Sale  
Cheshire, M33 3JN

t: 0845 224 8312  
f: 0845 224 7312  
e: [sales@intecpublicsector.com](mailto:sales@intecpublicsector.com)