



Violence Warning Markers

A policy and procedure guide

By

Tim Turner

CONTENTS

Author biography	2
1. Introduction.....	4
2. Summary.....	6
3. Legal background.....	8
4. Justifying the use of information.....	16
5. Setting up a system.....	19
6. What kind of system will you have?.....	21
7. What kind of warning are you going to share?.....	25
8. Triggers for a warning.....	28
9. Security of Information.....	31
10. Privacy impact assessment.....	34
11. Suggested process for setting up a database.....	35
12. Suggested flowchart for granting a warning.....	36
13. Procedural advice.....	37
14. Determining whether a warning is justified.....	38
15. Informing people and dealing with requests for information.....	41
16. Other rights and challenges.....	45
17. Sharing information externally.....	46
18. Other issues.....	48
19. Conclusion.....	50
Appendix 1: model system.....	51
Appendix 2: model policy.....	55
Appendix 3: model warning request form.....	61
Appendix 4: letter to person subject to warning.....	65
Appendix 5: DP compliance checklist.....	66
Appendix 6: The Slough Case.....	81
Appendix 7: The IC Guidance.....	84

LEGAL ADVICE

Data Protection and confidentiality law is a very complex area. The contents of this document are meant for you to consider as general guidance. It is not advice or opinion (legal or otherwise) on any specific system. You should obtain legal advice on specific issues from a qualified solicitor.

Any liability (in negligence or otherwise) arising from you acting or refraining to act as a result of anything in this document is excluded.

COPYRIGHT TERMS

Please note that a lot of time and effort has been invested in the preparation of this document. Tim Turner owns and asserts all copyright and moral rights. No part of this document may be reproduced, stored in an electronic retrieval system, emailed or published in any way (whether on the Internet or the Intranet) without the prior written permission of Tim Turner or ActNow Training.

However, where you have purchased an electronic version of this document on CD ROM, you have been granted a perpetual non-exclusive multi user license to:

1. Upload this document or any part of it onto your internal intranet site or portal for the sole use of your organisation's employees. In such cases you should add the following wording on the main page or some other prominent place:

© Tim Turner (2011) www.actnow.org.uk

This does not apply to the forms and policy contained in the appendices, which are supplied for you to adapt.

2. Make hard copies of this document for the sole use of your organisation's employees. You may also customise this document to suit your organisation. However the footnotes should not be altered as they show the origin of the document.

Under no circumstances should this document (electronic or paper version) be provided to any other person or organisation without the express written permission of the copyright owner (Tim Turner).

1. Introduction

Without a properly organised system for sharing warnings or alerts, warnings about threats and risks – real, exaggerated and imagined - will still be shared amongst staff. Free-text fields on databases will contain warnings and tip-offs. Incidents will be passed on informally. There will inevitably be gossip between staff, and even between staff and the public about what their neighbours are up to, or capable of. Even when using a central or corporate system, vital information will be missed. Some incidents will be unrecorded, or their significance underestimated. This is difficult to avoid. A lot will depend on how well you train your staff to avoid confrontations, and report serious incidents when they happen.

A central system for approving and circulating warnings allows the organisation to do as much as they can to ensure that the right information is available at the right time. Crucially, it allows warnings to be based on objective, verifiable evidence. A good quality, fair warning system should be part of a wider health and safety culture where incidents are recognised and investigated, and lessons learned in order that they can wherever possible be avoided. This guide is intended to help you to set up a safe, legal and effective system for sharing warnings and advice – you must ensure that it fits into the wider process of protecting staff and preventing incidents. Things can go wrong. In December 2010, Slough Council lost a case at the Court of Appeal ([2010] EWCA Civ 1171), and was found to have no defence for a widespread dissemination of warnings across their organisation. A tailored, focused approach was the one required by the Court (more information on the case can be found in Appendix 6).

The goal of your warning system must be staff safety. The design of your scheme must be geared towards providing advice to staff on how to protect themselves, other service users or clients, and the person. This may involve telling some staff about the nature of previous incidents (it may not), but it must always involve telling people what precautions they need to take. Health and Safety legislation is about protection not an arbitrary right to know, so whatever warning you provide, its purpose must be to protect staff and hopefully prevent further risk. Warnings are not about blame or punishment. A person whose behaviour gives rise to a warning may have personal or health issues that create the need for staff to be alerted. The amount of information used should be measured carefully, the audience for the warning carefully considered, and the language used to express the warning should be written with sensitivity as well as clarity.

As well as operating a warning system, we strongly recommend that you train your frontline staff routinely in conflict management and resolution. Tense situations that are diffused, and problems that are resolved amicably, no matter how frustrated or annoyed the subject might be at the beginning, benefit your organisation and the subject in equal measure. At

the same time as introducing a warning system, you should have adequate complaints mechanisms, well-trained customer contact staff, and where appropriate, mediation facilities or a way of accessing them.

This is not easy territory to traverse. The appropriate options may involve sharing less information than you think is necessary or justifiable. A one-size-fits-all approach will not succeed in complying with the law. Warnings must be tailored, and access must be measured and controlled. Operating a warning system of any kind involves constant vigilance and review. Senior officers have to take responsibility for ensuring that your system is fit for purpose, and remains so as time moves on.

The Act Now guidance

This guidance works in two parts. The main sections go through all of the issues that you have to consider when designing and implementing a warning system, or the issues you need to consider when reviewing a scheme that you already have in place. Throughout the guide, you will see certain parts highlighted in **yellow**. These are the most important pieces of advice we offer.

In the appendices, you will find a procedure for you to adopt as well as a description of a model scheme. We strongly recommend that you adapt the policy and model to suit your own needs.

There is one final point to make. This guide is written on the assumption that having evidence that a person poses a risk to your staff, you will have to keep dealing with them, going into their homes, speaking to them over the phone. It is also written on the assumption that the experts in much of this territory are those who work in risk management and health & safety, rather than data protection, and that the safety position should ultimately have the casting vote in any decision. It is entirely possible that experts in those areas will decide that the risk posed by a person means that a service or relationship with them has to be changed, restricted or withdrawn. Nothing in this guide should be taken to mean that you are obliged to continue to deal with people whom you genuinely believe are dangerous, or whose behaviour is unacceptable and cannot be tolerated. The guide does not go into this area purely because we assume that you will already have considered not dealing with the person at all.

2. Executive summary of the guide

- i. The purpose of a warning system is to protect staff – the amount and nature of information that is used should be balanced against the effect on staff safety.
- ii. Avoid publishing or circulating warnings information, especially by email or on notice boards – access to warnings or alerts should be controlled and measured. People at risk should be well informed; people unlikely to come into contact with even a dangerous person may well not need access to data.
- iii. Data Protection and Human Rights legislation is not set aside because a person has been violent or abusive – you need to be certain that interference with their rights or use of their information is justified and proportionate.
- iv. You must identify a safe, consistent and reliable source of information (or a group of sources) which will trigger a warning. The accuracy and reliability of trigger information is vital both to ensure warnings are effective, and that your system is legally robust.
- v. This guide starts from the position that the generation and use of warnings is a corporate (or at least) a department responsibility. Your organisation's most senior managers must approve the design of a warning system. In practice, decisions about the creation and issue of warnings should, in our view, be a corporate responsibility and should not be devolved to individual teams or managers. All of the advice in this guide is based on this recommendation.
- vi. **We strongly advise that you make it your policy that individual staff do not share warnings on your systems, but that they report them for proper consideration.** To protect staff safety, such reports should nevertheless be actively encouraged.
- vii. In principle, warnings or alerts will not be shared outside the organisation routinely – you will ensure that your system works well first, and look at the necessity and proportionality of sharing outside. It may be better to share only on request, or on a case-by-case basis.
- viii. The aim of this guide is to inform the creation of an organised warnings system. It may nevertheless sometimes be necessary to share information in an emergency e.g. there is credible evidence that a violent or dangerous person poses an immediate risk to one or more of your staff. Decisions may have to be made far faster than would normally be the case. Nevertheless, as long as those responsible for sharing information share information to those

at risk in good faith, it is extremely unlikely that the law will have been breached. You must record the reasons to use data outside the normal course of events.

ix. We strongly recommend that you fit your violence warnings system into a wider framework of policies and procedures. As a minimum, we suggest that you have the following items in place:

- An incident reporting system that allows staff to report violent or abuse-related incidents, and other risks to personal safety, supported by a process to investigate and manage them.
- A data protection, confidentiality & privacy policy which sets out your approach to using personal data.
- A procedure for reporting breaches of information security.
- A procedure or checklist to advise when to disclose personal data to third parties.