Checklist for setting up a warning database

- Develop a clear project initiation document, detailing why a system is needed, and how it will work. Questions that must be answered include:
    - Identify clearly where the information being used to develop warnings will come from
    - Identify objective and corporately agreed triggers
    - Set out procedures for ensuring data is fit for purpose
    - If a specific trigger like a violent incident report is not used (or is not the only trigger), determine which staff are entitled to nominate individuals to be the subject of a warning
    - Identify who will approve warnings

- Identify the audience for the warnings – why do they need warnings, and in what situations? What risks do they face, and what information do they need in order to keep themselves safe?

- Decide whether access will be granted to detail of incidents, and when

- Identify security arrangements, both for the central database and for access processes. Identify how inappropriate access will be identified, who will audit use of the system, and what the consequences of misuse will be.

- Identify the kind of approval / rejection process that will be used, and nominate roles for the approval of warnings.

- Carry out a data protection impact assessment and make any changes required before implementation

- Obtain approval from your board for the approach that you have taken

- Set out how the system works in a set of clear procedures

- Give briefings for all staff, explaining how the system works and what they must do

- Provide training for all users

- LAUNCH SYSTEM