DIGITAL SAFEGUARDING

AID116

Considerations to help protect victims of online stalking and domestic abuse.

Historic factors

- Does the perpetrator want to show the victim that they have some knowledge of their life and movements? If so, how?
- From what platforms does it appear they have gleaned information about the victim?
- Do they know about other conversations the victim has had with other people online?

Perpetrator's knowledge and capabilities

- What IT knowledge does the perpetrator have?
- Do they have access to the IT that the victim uses in their home (*e.g. internet provider)*?
- Do they still (or have they had) access to any IT device that the victim, their relatives or children still use? *(This might include routers, mobile phones, tablets, laptops and PCs.)*
- Do they have knowledge of the passwords, social media accounts, email addresses, platforms, numbers and any other individuals living with the victim *(especially those of any children)*?

DIGITAL SAFEGUARDING

AID116

Specialist knowledge or opportunity

- Who does the perpetrator work for?
- Does this job give them access to 'insider privilege'? For example, do they work for a mobile phone provider, communications company or internet service provider?
- Do they work for the IT department for the victim's employer?
- Do they have the programming skills to create mobile phone apps?
- Do they have the funds and/or the motivation to purchase private investigation skills from hackers /social engineers?

There is no one-size-fits-all advice to protect victims of stalking and domestic abuse. Be adaptable and flexible and take account of all the circumstances.

Appropriate safeguarding and protection will depend on the victim's lifestyle as well as the knowledge, tools, and tactics of the perpetrator.

Always signpost them to other help and support.

Have you identified any additional crimes which need to be recorded and investigated?