



The new Ofsted e-safety framework: is your school ready?

E-safety is constantly evolving, how you can keep up and empower children and teachers with the knowledge to identify and avoid online risks

New guidelines will ensure staff and pupils are educated in their use of technology, and have appropriate interventions and support in place should a particular issue arise.

From this September, Ofsted has issued new guidelines in regards to e-safety provision in schools. This basically means that during an inspection, Ofsted will be on the look out for how the school protects and educates staff and pupils in its use of technology, and what measures the school has in place to intervene and support should a particular issue arise.

As the framework is concerned with safeguarding pupils, it has to be a top priority for schools. Many schools might already have effective policies and systems in place, but those who haven't will need to revise their priorities to make sure this features. As a parent, I want to know that my children are safe in school, I want to know that they are empowered with the knowledge to be safe when they go online, and I want to know that staff have a good understanding of what safe means in any context to do with technology.

Many people I speak to get very wrapped up in blaming the technology as the facilitator of risk, but this really isn't the case. Risk and behaviour are the two fundamental principles of e-safety. In other words, if you don't know what an online risk is, your online behaviour can put you at risk.

Learning about e-safety is a vital life skill. Empowering children at an early age with the knowledge to safeguard themselves and their personal information is something that needs to be nurtured throughout school to see them into adult life. Equally it is important to empower adults, particularly parents, with the right information so that they can identify risky behaviour, or mitigate the possibility of risk.

The new Ofsted handbook and guidance have made the expectations that need to be met very clear. This is a summary of them:

- All teaching and non-teaching staff should be aware and able to recognise e-safety issues with high-quality leadership and management to make e-safety a priority

- High priority given to training and continuation training to all staff, including the contribution of the wider school community. One member of staff to receive accredited training (for example: to become an e-safety officer)
- Clear reporting processes
- Rigorous, plain English policies and procedures integrated with other relevant policies
- Progressive e-safety curriculum
- Provision of a recognised internet service provider (ISP) with age-related filtering
- Good risk assessment

While it does put an increased pressure on schools, particularly those that feel an e-safety assembly once a year is adequate, nobody can deny this new e-safety framework has been a long time coming. In an ever increasingly connected world, the risks to children have been growing as has the the risky (sometimes naive) behaviours of some children. The expectations are clear and the framework sets a fundamental building block for schools to empower their staff and children not only in school, but also outside of school.

So how do schools meet these expectations? You can't do everything at once and a plan of action and risk assessment should be your first step. This should clearly show any gaps in your e-safety provision and the priority of those gaps. Some things to consider in your plan would be:

- Have all staff, teaching and support, had adequate training? If so when was it and do they need an update? (I recommend annual updates). Training for the governing body and/or academy trust should also be considered
- Has that training incorporated a good awareness of all the e-safety risks and behaviours?
- Is e-safety embedded within the curriculum? If so does it incorporate all the risks?
- How is technology used in school, what different types of devices are capable of accessing online resources? Are those devices appropriately filtered and securely managed?
- Have there been any incidents, cyberbullying, for example, which would require reflection and retraining?
- Do staff take devices home? If so do those devices have personal information on them? If so are those devices encrypted?
- Is all of the above wrapped up in clear, plain English, including acceptable use policies that are age-appropriate? Are these policies read, understood and signed?

Of course, sometimes it's a case of "how do you know what you don't know?" This is understandable because like many things, e-safety is a vast area which is constantly evolving. Schools have an enormous responsibility and are continually fighting an uphill battle. There are many people out there who can help and a huge range of resources to call upon to prevent you from reinventing the wheel.

For further information see:

The Framework for Schools Inspections - this sets out the principles of inspections in schools in England, which includes academies. This is supplemented by briefings for use during inspections.
Schools Inspection Handbook - September 2012