E-safety & Ofsted inspection

According to Ofsted's School inspection Handbook, pupils need to feel safe at school and have to be "highly aware of how to keep themselves and others safe, **including in relation to e-safety."**

"Pupils are fully aware of different forms of bullying, including cyber-bullying and prejudice-based bullying, and actively try to prevent it from occurring. Bullying in all its forms is rare and dealt with highly effectively."

Inspectors should consider, "the effectiveness of safeguarding arrangements to ensure that...all pupils are safe. This includes...the promotion of safe practices and a culture of safety, including **e-safety."**

The Ofsted has outlined the following key features of outstanding practice:

Whole school consistent approach	All staff is fully aware of e-safety issues. E-safety is made a priority across all areas by the leadership and management team. Training is giving priority to increase understanding and build expertise in the area. The views of pupils, parents and the larger community are integrated.
Robust and integrated reporting routines	Reporting routes are in place and are widely understand and used by the school. Use of Report Abuse buttons, for example CEOP. Peer mentoring and support is available.
Staff	All staff are regularly trained on e-safety. Few members of staff have defined responsibilities and higher expertise in managing issues of safety.
Policies	E-safety policies covering processes and procedures are to be drawn by including the views of the whole school and approved by the governors. The e-safety policy should be linked to relevant policies like safeguarding, behavior and anti-bullying. It should include an Acceptable Usage Policy that is understood by pupils, staff and parents.
Education	A suitable curriculum must be drawn to engage pupils and teach them to take responsibility for their actions: it should teach pupils to stay safe, protect themselves from harm and take responsibility for others' safety. Awards and rewards may be used to encourage responsible use. Peer mentoring programmes may be put into place.
Infrastructure	Recognised Internet Service Provider (ISP) or Regional Broadband Consortium (RBC) together with age-related filtering that is actively monitored.
Monitoring and Evaluation	Data should be used effectively to monitor the impact of e-safety practice. E-safety must be promoted by undertaking regular risk assessments.

Management of Personal Data	Personal data must be managed securely and in accordance with the statutory requirements of the Data Protection Act 1998. Any professional communication that takes place through technology must be transparent and open to scrutiny, take place within explicit boundaries and must not be shared with young children.

Indicators of inadequate practice

- Children do not know how to report a problem.
- There is no staff training in place.
- Policies are outdated and generic.
- Personal data is unsecured.
- Poor password security.
- There is no in-depth e-safety education across the curriculum.
- There is no monitoring of the internet.

So, what does your school need to do?

- Develop an e-safety strategy by drawing from the views of parents and pupils.
- Provide adequate training to improve the knowledge and skills of staff while dealing with new technology.
- Work together with parents to ensure that technology is being used responsibly both at home and school.
- Deliver an e-safety curriculum in accordance with pupils' age so that they may become responsible users.
- Work with charities or providers to make sure that students are educated about e-safety.
- Review and monitor the e-safety policies and procedures by including frequent updates and addressing developments in technology.
- Help students understand the risks involved, both at school and at home, by efficiently managing the transition from a locked down system to a more managed system.