What to include in an e-safety policy for schools

Below are some key areas that should be included in a school e-safety policy.

The purpose and scope of the policy

For example:

- To educate pupils about e- safety issues and appropriate behaviours so that they remain safe and legal online.
- To help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.
- To keep any personal data and information secure.
- To minimise the risks of handling sensitive information.

Define different technologies
For example, websites, email, instant messaging, chat rooms, social media, mobile phones, blogs, podcasts, downloads, virtual learning platform.

Link to other relevant school policies
The e-safety policy should link to the schools acceptable use policy (for pupils and staff), policies for child protection, anti-bullying, and staff code of conduct.

Roles and responsibilities
For example, the Headteacher, Governing Body, E- Safety Co-ordinator.

Staff training
This should include details of e-safety training (which all staff should have attended) when the training should be refreshed and which members of staff have received accredited training.

Statements on Pupils with SEN
Pupils with SEN have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. The policy should outline the provisions the school will make to protect them.

A statement on how e-safety is covered in the curriculum
This should cover what children and young people are taught about e-safety and ICT in lessons and how e safety is embedded across the curriculum.

A statement on misuse of technology and breaching the policy
This should outline how the school will respond to misuse of equipment by pupils and staff.

How incidents are reported
How incidents/concerns should be reported and how they will be logged.

Parental involvement
For example:

- How parents are consulted about the policy.
- How the school involves them in promoting e safety.
- As part of the home school agreement, are parents asked to agree not to deliberately upload or text anything that would cause offence to anyone at school?

How images and film are managed

- Are parents asked to give consent for their child's image or work being uploaded on the school's website?
- How images of pupils are stored and for how long.

The management of email
The management of email accounts, password security, contact between staff and pupils via email, managing email accounts, what to do if you receive an offensive email, what happens if you send an offensive email.

Statement on passwords and password security
How passwords are kept secure and what happens if passwords are shared.

A statement on use of mobile technologies including mobile phones
When and how mobile phones can be used in school (including how they are used to support learning) and the sanctions for misuse of mobile phones.

Cover the use of webcams
For example:

- When and how webcams will be used in school.
- What measures the school takes to keep pupils safe when using webcams.
- The sanctions for misuse of webcams.

The use of video conferencing
This should cover when and how video conferencing will be used in school and what measures the school will take to keep pupils safe when using video conferencing.

Information on monitoring and evaluation
This should outline how the school will monitor the effectiveness of the policy and e-safety practices and update as necessary.

Further information on online safety in schools can be found in Annex C of Keeping Children Safe in Education (2016, DfE).