Ofsted requirements for e-Safety

e-Safety is now considered in the inspection of all education remits, including the early years sector, further education and skills and initial teacher education. Social care inspectors also consider e-Safety in the inspection of these remits, including in boarding and residential provision in schools and colleges, children's homes and adoption and fostering services and agencies.

e-Safety in schools

In the context of an inspection, e-Safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate. The breadth of issues classified within e-Safety is considerable, but can be categorised into three areas of risk: Content, Contact and Conduct.

Content

- Exposure to inappropriate content, including on line pornography; ignoring age ratings in games (exposure to violence, often associated with racist language); substance abuse and "revenge porn".
- Lifestyle websites, for example pro-anorexia, self-harm or suicide sites.
- Hate sites.
- Exposure to radicalisation/terrorism sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Cyberbullying.
- Identity theft, including "frape" (hacking Facebook profiles) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and on line reputation.
- Copyright (little care or consideration for intellectual property and ownership, such as music and film).
- Sexting (sending and receiving of personally intimate images).

The behaviour and safety of pupils at the school

The Ofsted Schools Inspection handbook, paragraph 174, requires inspectors to consider:

- Types, rates and patterns of bullying and the effectiveness of the school's actions to prevent and tackle all forms of bullying and harassment; this includes Cyberbullying and prejudice-based bullying related to special educational needs, sex, race, religion and belief, disability, sexual orientation or gender reassignment.
- The success in keeping pupils safe, whether within school or during external activities through, for instance, effective risk assessments, e-Safety arrangements and action taken following any serious incident.

The grade descriptor for ***outstanding*** includes:

- Pupils are fully aware of different forms of bullying, including Cyberbullying and actively try to prevent it from occurring. Bullying and derogatory or aggressive language in all their forms are rare and dealt with highly effectively.
- All groups of pupils are safe and feel safe at school and at alternative provision placements at all times. They understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations, including in relation to e-Safety.

The quality of leadership in, and management of, the school

Section 175 of the 2002 Education Act says "*The governing body of a maintained school shall make arrangements for ensuring that their functions relating to the conduct of the school are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school.*"

The Ofsted Schools Inspection handbook, paragraph 157, requires inspectors to consider:

- The effectiveness of the arrangements for safeguarding pupils who are educated wholly or partially off-site at a unit run by the school or at alternative provision.
- The promotion of safe practices and a culture of safety, including e-Safety.

The leadership and management of the school are likely to be judged to be ***inadequate*** if the school's arrangements for safeguarding pupils do not meet statutory requirements and give serious cause for concern, or insufficient action has been taken to remedy weaknesses following a serious incident.

Key features of effective practice

Whole School consistent approach

- All teaching and non-teaching staff can recognise and are aware of e-Safety issues.
- High quality leadership and management make e-Safety a priority across all areas of the school. Ideally, the school will have achieved a recognised standard, such as the e-Safety mark.
- A high priority given to training in e-Safety, extending expertise widely and building internal capacity.
- The contribution of pupils, parents and the wider school community is valued and integrated.

Robust and integrated reporting routines

- School based reporting routes that are clearly understood and used by the whole school (e.g. on line anonymous reporting systems).
- Report Abuse buttons (e.g. CEOP). Clear, signposted and respected routes to key members of staff.
- Effective use of peer mentoring and support.

Staff

- All teaching and non-teaching staff receive regular and up-to-date training.
- One or more members of staff have a higher level of expertise and clearly-defined responsibilities.

Policies

Rigorous e-Safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors.

The e-Safety policy could be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying

- The e-Safety policy should incorporate an Acceptable Use Policy that is understood and respected by pupils, staff and parents.

Education

- An age-appropriate e-Safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-Safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.
- Positive rewards are used to cultivate positive and responsible use.
- Peer mentoring programmes.

Infrastructure

- Recognised Internet Service Provider (ISP) or Regional
- Broadband Consortium (RBC).

Monitoring and evaluation

- Risk assessment taken seriously and used to good effect in promoting e-Safety.
- Using data effectively to assess the impact of e-Safety practice and how this informs strategy.

Management of personal data

The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.

Any professional communications that utilise technology between the school and pupils/students, their families or external agencies should take place within clear and explicit professional boundaries, be transparent and open to scrutiny and not share any personal information with a pupil.

Indicators of ineffective practice

- Personal data is often unsecured and/or leaves school site without encryption.
- Security of passwords is ineffective, for example passwords are shared or common with all but youngest children.
- Policies are generic and not updated.
- There is no progressive, planned e-Safety education across the curriculum (e.g. there is only an annual assembly).
- There is no internet filtering and monitoring.
- There is no evidence of staff training
- Children are not aware how to report a problem

Further e-Safety advice from Securus

If you find yourself confronted with an e-Safety concern that you don't feel equipped to manage, we may be able to help.

Our e-Safety advisors are able to discuss any safeguarding incidents or concerns you have. Our team can help you assess the situation and decide on the best course of action. They can also recommend ways of encouraging your pupils and staff to use technologies more safely.

If you are in any doubt about a capture please contact us and seek advice:

Securus Support email: **support@securus-software.com**

Securus Support telephone: **01372 388530**

LAN2LAN House, Brook Way, Leatherhead, Surrey, KT22 7NA, United Kingdom

t: +44(0)330 124 1750 e: customer.services@securus-software.com

Registered in England No. 4613837