**Online Safety Checklist** **for Schools and Colleges** – Jo Brown August 2018

This checklist is based on the South West Grid for Learning award winning 360 Safe Tool <http://www.360safe.org.uk/Home> and reference to Keeping Children Safe in Education (KSIE) (including September 2018 version) It is recommended that you sign up for the 360 Safe tool for a comprehensive online safety self-evaluation and system for improvement. This will also support you to meet Ofsted expectations and KSIE requirements. Please refer to the <https://360safe.org.uk/Overview/PDF-Version> for a more comprehensive checklist/view of the tool content.

KSIE states that all staff should undergo safeguarding and child protection training on induction, including online safety and that this training should be regularly updated. It also states that “governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place” in relation to internet access. KSIE 2018 adds that schools must recognise children may be accessing internet via phones and as well as appropriate monitoring and filtering need to have a policy about children accessing internet whilst at school.

KSIE 2018 also states that policies should include how the school deals with peer on peer abuse, how the risk of peer-on-peer abuse (including sexting) is going to be minimised, and how these incidents are recorded, investigated and dealt with. The national sexting guidance [Sexting in Schools and Colleges 2017](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf) and 1 page [Overview\_of\_Sexting\_Guidance.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/647389/Overview_of_Sexting_Guidance.pdf)should therefore be referred to.There is specific reference to the online components of sexual violence and sexual harassment (including sexting) and the relevant

[guidance](https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges) should be referred to.

**Additional Oxfordshire resources and links**. Latest versions will be available on <http://schools.oxfordshire.gov.uk/cms/content/policy-and-guidance> and <http://schools.oxfordshire.gov.uk/cms/content/internet-safety-and-cyberbullying>

E-safety cyberbullying toolkit

Managing youth produced sexual imagery – sexting resource pack

CLICK Resource pack (primary schools) [Click - online safety, cyberbullying and digital resilience](https://fisd.oxfordshire.gov.uk/kb5/oxfordshire/directory/advice.page?id=9nGKyaZoCUI)

OSCB Digital Safeguarding Training can be accessed via <http://www.oscb.org.uk/themes-tools/e-safety/>

|  |  |  |
| --- | --- | --- |
| **Policy and Leadership** | | |
| 1. Who is responsible for E-safety? Do you have an E-safety Co-ordinator, an active e-safety committee including all stake holders and are governors involved in developing policy and monitoring of incidents? | Yes/no/partial | Action needed |
| 1. Do you have a comprehensive e-safety policy? Does the policy link to all other relevant policies (Anti-Bullying, Peer on Peer abuse; child protection etc.) (*note KSIE 2018 requirements)* |  |  |
| 1. Is there guidance for Acceptable Use in place, appropriately differentiated and regularly reinforced? |  |  |
| 1. Is E-safety part of self-evaluation and linked to other relevant policies e.g. behaviour policy, Anti-Bullying policy, ICT policies, safeguarding etc. |  |  |
| 1. Are their strategies for management of unacceptable use, clearly understood by all and that cover behaviour beyond school? Are these regularly reviewed and updated? |  |  |
| 1. Are their clear policies in relation to mobile phones, digital images, use of communication technologies (e-mail, chat, blogs, etc.) school website/learning platform? |  |  |
| 1. Are there clear protocols, professional standards in place regarding communication of staff with other members of schools and wider community? |  |  |
| **Infrastructure** | | |
| 1. Are their clear policies in relation to passwords and are passwords secure? Are they age-appropriate for students and reinforced via the curriculum? |  |  |
| 1. Is the school’s internet service provided by a recognised ISP with filters and monitoring? Is illegal content filtered by actively employing illegal content lists? Does it include mechanisms to protect users from extremist/terrorist material? (prevent agenda)   *Are there policies in place re children accessing internet via their phones (KSIE 2018)* |  |  |
| 1. Do school systems meet technical security requirements? |  |  |
| 1. Are their clear policies in place regarding personal data understood by all stakeholders? |  |  |
| **Education** | | |
| 1. Is there a planned e-safety education embedded in all aspects of the curriculum including protecting vulnerable learners? Does it involve young people as peer educators? |  |  |
| 1. Are pupils taught about information literacy including developing skills for safe and discriminating online behaviour? |  |  |
| 1. Are young people’s skills recognised and are they involved in e-safety education? |  |  |
| 1. Is there a planned programme of formal e-safety staff training that is regularly reviewed and integral to child protection/safeguarding training? (*Meets KSIE 2018)* |  |  |
| 1. Is e-safety awareness training provided for Governors? |  |  |
| 1. Are parent/carers provided with opportunities for training, information and know who to contact if concerned? |  |  |
| 1. Does the school provide opportunities for members of the wider community to gain information and understanding about e-safety? |  |  |
| **Standards and Inspection** |  |  |
| 1. Is there recording, monitoring and reporting of online safety incidents? *Does this include peer on peer and have KSIE 2018 requirements been considered?* |  |  |
| 1. Is e-safety policy and practice monitored and reviewed? |  |  |