***Keeping Children Safe in Education***

***E-safeguarding Mapping***

This document maps any references to e-safeguarding within the Keeping Children Safe in Education and offers some advice on what good practice might be.

|  |  |  |  |
| --- | --- | --- | --- |
| Reference | Para. | Suggested good practice | Actions  (For school use) |
| Every school and college should have a designated safeguarding lead who will provide support to staff members to carry out their safeguarding duties and who will liaise closely with other services such as children’s social care. | 8 | As e-safety is part of safeguarding then there should be a designated lead. It might be that it is the one and same person.  It is good practice to add posters around school to show who the lead and deputy is.  Ensure that all staff are aware of who this lead is. |  |
| All staff members should receive appropriate safeguarding and child protection training which is regularly updated. In addition all staff members should receive safeguarding and child protection updates (for example, via email, e-bulletins and staff meetings), as required, but at least annually, to provide them with relevant skills and knowledge to safeguard children effectively. | 13 | Ensure that e-safety is integral in the safeguarding training. It is suggested that at least an annual training update is scheduled. This could include any emerging technologies. |  |
| **Record keeping**  All concerns, discussions and decisions made and the reasons for those decisions should be recorded in writing. If in doubt about recording requirements, staff should discuss with the designated safeguarding lead. | 29 | All e-safety issues should be recorded (sample template is available from the LA team) |  |
| Sexual abuse: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse (including via the internet). Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children. | 39 | Information only. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Reference | Para. | Suggested good practice | Actions  (For school use) |
| **Safeguarding Policies**  Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare.  This should include:  • an effective child protection policy; and  • a staff behaviour policy (sometimes called the code of conduct) which should amongst other things include - acceptable use of technologies, staff/pupil relationships and communications including the use of social media  These policies, along with Part one of this guidance (Keeping children safe in education) and information regarding the role of the designated safeguarding lead, should be provided to all staff on induction | 47/48 | There should be a mention of e-safety within your safeguarding policy and good practice to have a separate E-Safety policy.  All users should have signed acceptable use policies.  The staff behavior policy should refer to acceptable use policies and should refer to staff use of social media, including reference to staff/pupil relationships within social media. |  |
| The designated safeguarding lead and any deputies should undergo training to provide them with the knowledge and skills required to carry out the role. The training should be updated every two years | 57 | Designated leads to attend more in depth e-safeguarding training. One such area might include CEOP training |  |
| **Staff training**  Governing bodies and proprietors should ensure that all staff members undergo safeguarding and child protection training at induction. The training should be regularly updated. Induction and training should be in line with advice from the LSCB.  In addition all staff members should receive regular safeguarding and child protection updates (e.g. via email, e-bulletins, staff meetings) as required, but at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.  Governing bodies and proprietors should recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns on a daily basis. Opportunity should therefore be provided for staff to contribute to and shape safeguarding arrangements and child protection policy. | 64/65/66 | Induction training should include e-safety training within the safeguarding element.  Annual refresher training (as outlined earlier) |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Reference | Para. | Suggested good practice | Actions  (For school use) |
| **Online safety**  As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place.  Additional information to support governing bodies and proprietors is provided in Annex C | 67 | Schools should have a robust filtering solution in place (Schools following the LA solution have this inn place).  Schools should have a robust monitoring solution in place (schools following the LA solution have this in place). |  |
| **Opportunities to teach safeguarding**  Governing bodies and proprietors should ensure children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through personal, social, health and economic education (PSHE), tutorials (in FE colleges) and/or, for maintained schools and colleges, through sex and relationship education (SRE).  Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding. | 68/69 | Schools should have a broad and balanced e-safeguarding curriculum where pupils are taught of the risks and safe practice when age appropriate.  Filtering solution is flexible enough to be customized when required and is not locked down. (schools following the LA solution have this in place).  Filtering changes should be possible but only carried out with proper authority and are fully documented. (LA template is available) |  |
| Peer on peer abuse can manifest itself in many ways. Governors and proprietors should ensure sexting and the school or college’s approach to it is reflected in the child protection policy. The department provides searching screening and confiscation advice for schools. The UK Council for Child Internet Safety (UKCCIS) Education Group has recently published sexting advice for schools and colleges. | 77 | The school’s approach to sexting should be reflected within the child protection policy. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Reference | Para. | Suggested good practice | Actions  (For school use) |

|  |  |  |  |
| --- | --- | --- | --- |
| **Further information on preventing radicalisation**  Protecting children from the risk of radicalisation should be seen as part of schools’ and colleges’ wider safeguarding duties, and is similar in nature to protecting children from other forms of harm and abuse. During the process of radicalisation it is possible to intervene to prevent vulnerable people being radicalised. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism.  There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer. The internet and the use of social media in particular has become a major factor in the radicalisation of young people. | Annex A | A thorough monitoring solution is an aide to identifying any trends arising.  Schools should have a robust monitoring solution in place (schools following the LA solution have this in place). |  |
| Schools should ensure that children are safe from terrorist and extremist material when accessing the internet in schools. | Annex A | Schools should have a robust filtering solution in place (schools following the LA solution have this in place). Schools should have a robust monitoring solution in place (schools following the LA solution have this in place). |  |
| The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.  The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk: • content: being exposed to illegal, inappropriate or harmful material;  • contact: being subjected to harmful online interaction with other users; and  • conduct: personal online behaviour that increases the likelihood of, or causes, harm | Annex A | For information |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Reference | Para. | Suggested good practice | Actions  (For school use) |

|  |  |  |  |
| --- | --- | --- | --- |
| Filters and monitoring Governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the above risks from the school or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school/college has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks. The appropriateness of any filters and monitoring systems are a matter for individual schools/colleges and will be informed in part by the risk assessment required by Prevent Duty.  The UK Safer Internet Centre has published guidance as to what “appropriate” might look like:  • UK Safer Internet Centre: appropriate filtering and monitoring | Annex A | Schools should have a robust filtering solution in place which allows for age appropriate profiles (schools following the LA solution have this in place). |  |
| Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school approach to online safety. This will include a clear policy on the use of mobile technology in the school.  Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises.  Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding. | Annex A | Schools should consider other ways that children may access the internet in school, including through personal devices. Schools should have looked at assessing risk with the management of this.  Good practice to have this documented.  Suggested that there is a Mobile Phone Policy. Inspectors have asked for this. |  |
| Staff training Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 64) and the requirement to ensure children are taught about safeguarding, including online (paragraph 68), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach. | Annex A | Regular staff training programme. |  |