Writing an Online Safety Policy

Guidance and resources for Educational Setting Leaders, Managers and Designated Safeguarding Leads

September 2017 (updated May 2018)

Writing an Online Safety Policy: Guidance for Educational Settings

This document contains guidance for leaders, managers and Designated Safeguarding Leads (DSLs) within educational settings, to help them develop an appropriate online safety policy.

It is recommended that this document be read **before** accessing the Kent online safety policy template.

This document has been produced by the Kent Education Safeguarding Team with input from children and young people, schools, multi-agency children's workforce professionals, Kent Safeguarding Children Board (KSCB) and Kent Police.

Who is the document for?

This guidance has been developed for all educational settings including, but not limited to; schools, early years settings, Pupil Referral Units (PRUs), 14-19 settings, further education colleges, alternative curriculum provisions and hospital schools etc. The terms 'school' or 'pupils' may appear within this document, but it is still relevant and appropriate for other educational settings.

Questions and queries

If Kent educational settings wish to discuss this document, or any other online safety concerns, please contact the Kent County Council's Education Safeguarding Adviser (Online Protection) or e-Safety Development Officer.

Please note this document was updated in May 2018 to include references to GDPR.

Contents

.

Policy Aims and Scope

What is meant by 'Online Safety'?

Online safety or "e-Safety" is part of the safeguarding 'duty of care', which applies to everyone working with children and young people; it includes education on the safe and responsible use of technology, as well as, the policies, procedures, risk assessments and infrastructure that are implemented in order to safeguard the whole school community when accessing the internet and associated technologies.

It should be noted that the term 'online safety', rather than 'e-Safety', should be used to reflect the wide range of issues associated with technology; meaning that online safety should be regarded more as a safeguarding concern, rather than an ICT issue.

What are the main online safety risks that educational settings need to be aware of?

Children, young people, and indeed adults, may encounter a range of risks online; these are identified within Annex C of 'Keeping Children Safe in Education' (KCSIE) 2016 as the three C's:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

This could include:

	Commercial	Aggressive	Sexual	Values
Content	• Advertising & Sponsorship • Spam • Copyright	• Violent content • Hateful Content	• Pornographic content • Sexual comments	• Racist & extremist content • Misleading or biased information & advice • Body image & self esteem • Distressing or offensive content
Contact	• Tracking • Geo-location • Harvesting data	• Being bullied (cyberbullying), harassed or stalked	• Meeting 'strangers' • Sexualised bullying • Grooming • Online Child Sexual Exploitation	• Self-harm & suicide • Unwelcome persuasions • Grooming for extremism
Conduct	• Sharing personal information • Illegal downloading &/or sharing • Hacking • Gambling	• Bullying (cyberbullying), harassing or stalking others	• Sexualised bullying of others • Sharing sexual content • Creating or sharing Youth produced sexual imagery (Sexting) • Unhealthy/inappropriate sexual relationships • Child on child sexualised or harmful behaviour	• Providing misleading or biased information & advice • Encouraging others to take risks online • Sharing extremist views • Creating &/or sharing inappropriate content • Problematic Internet Use or "Addiction" • Plagiarism

Content adapted from EU Kids Online 2008

What does the national guidance for educational settings say about online safety?

Educational settings have specific, statutory responsibilities to ensure and promote children's safety and well-being; this also applies to the online environment.

The statutory government guidance which highlights this for educational settings includes; Keeping Children Safe in Education (2016), Early Years and Foundation Stage (2017), Preventing and Tackling Bullying (July 2017), Screening, Searching and Confiscation (February 2014) and The Prevent Duty (July 2015).

Keeping Children Safe in Education 2016

'Keeping Children Safe in Education' 2016 (KCSIE) is statutory guidance from the Department for Education (DfE) which applies to all schools and colleges. Educational settings must comply with KCSIE when carrying out their duties to safeguard and promote the welfare of children, unless exceptional circumstances arise.

The specific responsibilities, regarding online safety; include, but not limited to:

- A requirement for an effective child protection policy in place, together with a staff behaviour policy (code of conduct/Acceptable Use Policy) which includes staff/pupil relationships and communications including the use of social media;
- All staff are aware of the role of technology within abuse;
- All staff recognise that abuse can be perpetrated by children themselves; and appropriate policies and procedures in relation to peer on peer abuse, including 'sexting' and cyberbullying are in place;
- Ensuring that children are taught about online safety, through a variety of teaching and learning opportunities, as part of providing a broad and balanced curriculum
- All members of staff receive appropriate online safety training;
- That leaders and managers ensure there is appropriate filtering and monitoring in place.

A more detailed summary of the specific online safety points, considerations and suggested actions can be found on Kelsi.

Early Years Foundation Stage 2017

The Early Years Foundation Stage framework (EYFS) 2017 sets the standards for learning, development and care for children from birth to five.

The specific responsibilities, regarding online safety; include, but not limited to:

- Educational programmes must guide children to make sense of their physical world and their community; including the use of technology.
- Safeguarding policies must cover the use of mobile phones and cameras within the setting.
- All staff should be trained to recognise inappropriate behaviour displayed by other members of staff, including inappropriate sharing of images.

EYFS 2017 also suggests that childcare providers may find it helpful to refer to 'Keeping Children Safe in Education' 2016; although this is not statutory, it is recommended that providers refer to this guidance, particularly if they allow access to the internet and technologies within the setting.

Ofsted

All educational settings should be mindful of Ofsted's expectations regarding online safety, identified within the 'Common Inspection Framework' (CIF), 'Inspecting Safeguarding' briefing and other supporting documents.

Online Safety is specifically referenced in the 'Inspecting Safeguarding' briefing within a range of areas, most explicitly within section 13, 'The signs of successful safeguarding arrangements':

- ...'*Adults understand the risks posed by adults or learners who use technology, including the internet, to bully, groom, radicalise or abuse children or learners. They have well-developed strategies in place to keep children and learners safe and to support them to develop their own understanding of these risks and in learning how to keep themselves and others safe. Leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children's well-being. Leaders of early years settings implement the required policies with regard to the safe use of mobile phones and cameras in settings.'*

More in depth information regarding Ofsted and online safety can be found on Kelsi.

Why should educational settings have an online safety policy and what should it cover?

An Online safety policy provides educational settings with a framework to develop their online safety ethos, and enables leaders and managers to detail strategic approaches and considerations, with regards to the safer use of technology. This could include, but is not limited to:

- Acceptable use of technologies
    - Including staff/pupil relationships and communications using social media
- Use of mobile phones, cameras and personal devices
- Procedures for responding to online abuse, including peer on peer abuse
- Educational and engagement approaches across the community

The Online safety policy should be recognised as a safeguarding policy, not a technical or ICT policy.

There is no requirement to have a separate policy, if online safety issues are appropriately addressed within other existing policies; this decision will be down to individual educational setting's leaders and managers. If online safety is embedded within existing documents, settings should ensure that their community is aware of how and where to locate specific online safety information, especially regarding responding to and reporting concerns.

What other policies should include online safety information?

The Online safety policy will need to be interlinked with many different policies including, but not limited to:

- Anti-bullying policy
- Acceptable Use Policy (AUP) and/or the Code of conduct
- Behaviour and discipline policy
- Child protection policy
- Confidentiality policy
- Data security/information governance
- Image use policy
- Searching, screening and confiscation policy

Online safety should also be specifically identified within appropriate curriculum policies including Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE). This will enable educational settings to evidence that children receive online safety teaching and learning opportunities as part of a broad and balanced curriculum.

Can educational settings adapt the Kent template policy statements?

Yes. We encourage all educational settings to ensure that their online safety policy is individualised for their own specific context, to ensure it is fit for purpose.

It would not be appropriate for educational settings to simply adopt the Kent template in its entirety, as some statements will be more relevant to particular settings than others; for example, one early years setting may not have internet access on site, whilst another provides children with 1:1 tablets.

Similarly, the online safety policy template requires leaders, managers and DSLs to adapt the content to include specific information, such as procedures and expectations; these decisions will vary from setting to setting, so the template should be used as a starting framework.

How could educational settings involve the community in developing online safety policies?

Educational settings should view online safety as a whole setting issue and implement a holistic approach to writing and updating the policies. The more that staff, parents, governors and pupils are involved in deciding and creating the policy, the more effective it will be in the long term, by ensuring a sense of ownership is developed.

Members of staff from a variety of roles and experience should be asked to contribute to the policy, including: curriculum leads, technical staff and specialist roles such as SENCOs, to ensure that educational, strategic and technical issues are all considered.

Educational settings may find it easier to share policies with a smaller working group of parents and/or pupils, rather than the setting community as a whole; working with existing groups, such as: key stage leaders, pupil councils or parent associations may be a helpful starting point. Some educational settings have developed this further by encouraging such groups to develop pupil and/or parent ‘friendly’ policies.

Children and young people are more likely to be aware of new developments within technology and may be able to provide educational settings with an excellent way of keeping up-to-date with the rapidly changing pace of development, especially within social media and the associated apps and games.

Monitoring and Review

How often should educational settings review their online safety policy?

The Online safety policy should be reviewed at least annually, in line with the safeguarding policies. In actuality, the Online safety policy should be regarded as a 'live document' and should be revised following:

- Any local or national guidance or legislation changes
- Specific online safety concerns or incidents within the community
- The introduction of new technology and systems within the setting

This could mean that policies are revised several times throughout the year; whilst this may seem to be a time consuming task, it's unlikely that significant rewrites will be required each time and will ensure that the setting is compliant with statutory guidance and safeguarding their community effectively.

To keep up-to-date and receive communications from the Kent Education Safeguarding Team regarding online safety guidance, then managers, leaders and DSLS can subscribe to the Kent online safety blog.

How can educational settings monitor the impact of their online safety policies?

Leaders and managers, including Governors or other strategic bodies such as trusts, boards or committees should take an active role in monitoring the impact of their policies.

This may include:

- Implementing a systematic and regular review of online safety policies
- Meeting with the DSL to review responses to specific incidents or concerns
- Evaluating impact of engagement approaches

Tools to support management and leadership teams to do this include:

- The Kent Online Safety Self-evaluation tool (available on the Kelsi website)
- South West Grid for Learning 360 safe tool.

Roles and Responsibilities

What are the key responsibilities for leaders and managers?

Leaders and managers have a range of statutory responsibilities as identified within annex C of KCSIE 2016. Leaders and managers must ensure that are aware of safe practice expectations and should proactively seek advice and support when developing their online safety approaches. The management and leadership team will have ultimate responsibility for any online safety incidents that may occur whilst on site; a lack of knowledge of online safety or technology is no defence.

To support Governors to explore and develop online safety practice within their schools, the UK Council for Child Internet Safety (UKCCIS) education group have published: "Online safety in schools and colleges: Questions from the Governing Board".

Why is online safety within the role of the Designated Safeguarding Lead?

KCSIE highlights online safety as a safeguarding concern; therefore the ultimate responsibility for online safety falls within the remit of the Designated Safeguarding Lead (DSL).

Some online safety incidents will reach the threshold for child protection action; the online safety lead must have a robust understanding of local safeguarding procedures. It will therefore not be appropriate another member of staff to lead on online safety incidents, unless they have been trained to an equivalent standard to enable them to act as a deputy DSL.

The DSL does not need to have vast technical knowledge, as online safety is a safeguarding, not technical role. Staff with appropriate skills, interest and expertise, regarding online safety should support the DSL as appropriate, for example when developing curriculum approaches or informing technical decisions.

Further information on the role and responsibilities of the DSL, including information on online safety groups, can be found in 'The Role of the Online Safety Lead in Education Settings: Guidance for Leaders and Managers' available on Kelsi.

What are the key online safety responsibilities for staff?

Members of staff play an essential role in creating a safe culture, they are also likely to be the first point of contact for online safety incidents, or be in a position to identify behaviour changes which could indicate that an individual is at risk of harm.

The Online safety policy will only be effective with staff if they subscribe to its principles and methods; staff should be given opportunities to discuss any issues the policy raises and explore appropriate teaching strategies.

Where staffing functions are provided by external contractors or services; educational settings should take steps to ensure that contracted staff support the settings online safety ethos and adhere to the online safety policy and practices. It would be unreasonable, for instance, if supply staff were asked to take charge of an internet activity without adequate understanding of the educational settings policy and procedures.

What needs to be considered with regards to staff managing the technical environment?

Members of staff responsible for managing the technical environment have an essential role to play in establishing and maintaining a safe online environment; they should work closely with the leaders, managers and DSLs, as well as pastoral and curriculum staff, to provide expertise relating to appropriate

use of ICT systems and to ensure that learning opportunities are not unnecessarily restricted by technical safety measures.

Technical staff will need clear supervision and support in their roles by the leadership and management team (including DSLs) and, along with all staff, will require regular training and professional opportunities to enable them to remain up-to-date with emerging online safety issues.

Technical staff should follow the setting's procedures if they discover, or suspect, online safety concerns through monitoring of network activity. They should also be aware of how to report concerns to the DSL and/or headteacher/manager in line with existing safeguarding policies, including: Allegations, Child protection and Whistleblowing.

If an educational setting outsources their technical, it is important that the service provider understands, supports and upholds the setting's online safety practices and takes appropriate steps to minimise risks. There needs to be clear reporting procedures in place, regarding breaches of system or network security, to ensure the educational setting (e.g. the DSL and/or the headteacher/manager) can take appropriate internal action to safeguard the community.

What are the key online safety responsibilities for children?

The responsibility that children and young people have, in relation to their own online safety, should not be underestimated. Children should be encouraged and empowered to develop safe and responsible online behaviours, over time, to enable them to manage and respond to online risks as they occur.

Children and young people should be given a role in developing the online safety policy; if children feel that their views have been heard (and therefore understand some of the issues affecting the decisions), settings may find that they are more inclined to abide by the rules.

What are some of the key online safety responsibilities for parents and carers?

Parents and carers play a crucial role in developing children's safe and responsible online behaviours, especially as the majority of their access to technology occurs off school site.

Parents and carers have a responsibility to work in partnership with education settings to reinforce online safety messages and to role model, promote and encourage safe online behaviours, wherever and whenever children use technology.

As with children and young people, parents and carers should be involved in the development of the policies to help build and develop a shared approach to safeguarding children online, both at school and at home.

Education and Engagement Approaches

How should educational settings educate and engage children?

KCSIE highlights that governing bodies and proprietors need to '…*ensure that children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum which may include covering relevant issues through personal, social, health and economic education (PSHE), tutorials (in FE colleges) and through sex and relationship education (SRE*)' (Section 68).

Online safety education for children needs to explore a range of skills. This will include:

- The importance of using technology safely and respectfully
- Understanding implications regarding sharing of personal information
- Identifying where to go for help and support if they have concerns about content or contact on the internet
- Digital literacy skills to refine their own publishing and communications with others
- Respect for copyright and intellectual property rights and the correct use of published material.
- Critical awareness of the dangers and consequences of plagiarism, copyright, piracy, reliability and bias.
- Developing an understanding on how to become safe and responsible online citizens
- Positive, healthy and age appropriate online relationships

Whilst the computing curriculum and assemblies will, no doubt, form an essential part of pupil's online safety education, the best approach is to implement a progressive programme, across the curriculum, which allows children to develop appropriate strategies to respond to online risk. Online safety education should be reinforced whenever pupils are using the internet; therefore a computing or one off assembly only approach will not be robust.

Children need to develop a broad understanding of safe and responsible online behaviour and relationships; therefore content within the Personal Social and Health Education (PSHE) and Sex and Relationships (SRE) curriculum will be required.

Some useful online safety programmes include:

- Think U Know
- Childnet: Including
    - Kidsmart
    - PSHE Toolkit
    - Smartie the Penguin
    - The adventures of Kara Winston and the Smart Crew
    - Digiduck's Big Decision
    - Know it all: Secondary toolkit
- Digital Literacy Scheme of Work
- Internet Matters
- BBC
    - Webwise
    - CBBC
    - BBC Bitesize – Computing and PSHE

A vast range of other suggested curriculum links and resources to use with children from early years to sixth form/college provision can also be found on Kelsi.

Kent County Council has also produced posters with online safety acceptable use suggestions which are available to download and display, to remind children of responsible online behaviour and expectations.

What should educational settings consider with regards to vulnerable children?

Children and young people may be considered to be vulnerable for a variety of reasons, including: children with Special Education Needs and Disabilities (SEND) and/or mental health needs; children in care; children who have experienced trauma or abuse; children with low self-esteem; children who have English as an additional language; and children who are considered to be vulnerable on a temporary basis, due to personal or specific circumstances.

Vulnerable children will have individual needs that present a range of issues when teaching online safety; some common difficulties may include;

- Lack of social awareness and understanding
- Naivety or lack of trust
- Transferring skills or concepts
- Unable to verbalise concerns
- Some children may have poor recall and difficulties with learning through experience.
- Disrupted or traumatic childhood
- Poor attachments
- Lack of boundaries
- Poor understanding of risk

The SENCO and members of the pastoral team should be involved in developing and reviewing the Online safety policy, to provide a specialist perspective and synchronise support, to ensure the needs of vulnerable pupils are being met.

Further guidance with specific considerations regarding online safety and children with SEND can be found on Kelsi.

How should educational settings train and engage staff?

Online safety training for staff should be integrated and aligned with the educational setting's overarching safeguarding approach; it should be updated, at least, annually, as part of whole school training and development, not just a reactive approach, following an incident or concern.

All staff, including: administration, midday supervisors, caretakers, governors and volunteers, not just teaching staff, should be included in online safety awareness training; a child may disclose online safety concerns to any member of staff, so it is essential that all staff are able to recognise possible risks and know how to respond.

Additionally, all members of staff should be given clear information regarding the settings expectations in relation to acceptable use of technology, including staff/child relations and use of social media, in order to safeguard themselves from allegations, as well as protecting children from potential abuse.

Induction of new staff, including volunteers, should always include a discussion about the Online safety policy and Acceptable use policy.

Leaders, managers and DSLs should attend, facilitate and support online safety training for staff, to ensure that messages are appropriate and consistent; this also demonstrates that online safety is viewed as a priority by leadership.

It is recommended that DSLs ensure that staff:

- Are aware of the settings online safety policy and specific safe practice expectations
- Are able to recognise the potential risks posed by the internet, including cyberbullying, 'sexting', online sexual abuse/exploitation and inappropriate content (including underage use of social networking)
- Understand the need to report and record online safety concerns in the same way as other safeguarding issues
- Are aware of how to respond to online safety concerns, including cyberbullying and 'sexting' and allegations against members of staff. They should be aware of how to refer issues both internally and externally
- Are aware of professional behaviour online, its potential implications and an understanding of appropriate use of technology, including the use of social media
- Are aware of useful resources to embed the online safety curriculum and to protect the whole community online

The Kent Education Safeguarding team, via the Education Safeguarding Adviser (Online Protection) and e-Safety Development Officer can provide support for DSLs or can commissioned to deliver bespoke online safety training for staff.

How should educational settings raise awareness with and engage parents and carers?

Parents and carers are vital to teaching and empowering children to become safe and responsible digital citizens.. Educational settings should ensure that online safety messages are shared and promoted with parents to ensure that a partnership approach is established.

Educational settings may be able to educate parents about online safety through workshops or parent awareness sessions and help them plan appropriate, supervised use of the internet at home. It is important that settings focus on the importance of parenting skills to keep children safe online, so that online safety is not seen as a purely IT issue.

It is unlikely that all parents will be able to engage with one off events, so education settings should provide information regarding online safety through a variety of channels; this could include: the setting's website, newsletters and social media channels, as well as creative ideas, such as: inviting parents to attend performances or events facilitated by their children.

Further information, including ideas and supporting resources, to help educational settings engage families in online safety can be found on Kelsi.

Reducing Online Risks

How can educational settings reduce online safety risks?

Many emerging technologies offer the potential to develop teaching and learning. New applications are continually being developed and changing which can offer immense opportunities for socialisation and learning, as well as increasing online safety risks, for example pupils using a phone to video a teacher's reaction in a difficult situation. It is essential that the use of technology is carefully managed by educational settings to ensure that all members of the community are kept safe and that online risks and dangers are recognised by the setting and mitigated.

A risk assessment should be undertaken on each new technology so that effective and safe practice can be developed. The safest approach will be to deny access until a risk assessment has been completed and safety and appropriate action has been established and taken.

Leaders and managers will need to keep up to date with new technologies and be ready to develop appropriate strategies. For instance instant messaging via mobile phones is a frequent activity for many pupils and families; this could be used to communicate an absence or send reminders for exam coursework. There are dangers for staff however if personal phones are used to contact pupils and therefore a school owned phone or communication channel should be issued.

Risks can be considerably greater where tool are used which are beyond the settings control such as most popular social media sites. Specific guidance and considerations for schools around this topic (including a checklist and sample risk assessment templates) can be found in the "Using Social Media in Educational Settings" document.

Safer Use of Technology

What considerations do leaders and managers need to make regarding safe use of technology within the classroom?

Technology is a fantastic tool for teaching and learning, however it can bring safeguarding and reputation risks if safer classroom practice is not established.

Classroom Management

Educational settings should consider the following points to develop safe and responsible use of technology with children:

- Staff must not rely on filtering alone to safeguard children from harm online; supervision and good classroom management is essential when using any form of technology
    - Boundaries and acceptable behaviour should be discussed with children prior to internet access.
- Staff should always role model safe and appropriate behaviour when using technology.
- The decision to use technology (including websites, apps and devices) with children, must be made based on a risk assessment approach

- Websites, apps and devices should be evaluated fully, before use in the classroom - this will include testing the websites first, pre-checking search results, and reviewing website terms and conditions.
- Particular attention should also be paid to advertisements, as they can change each time a web page or app is accessed and what may be considered appropriate today, might not be tomorrow!

Despite all these measures, children may still be exposed to inappropriate content; leaders must ensure that there are clear procedures for reporting unsuitable content, which are understood by staff and children.

Safer Searching

The decision, regarding which search tools to use, will be for individual educational setting to consider following an appropriate risk assessment; leaders and managers should weigh the educational benefits against the possible safeguarding concerns. Leaders should also consider the possible negative impact on pupil's education if they are unnecessarily restricted from appropriate online resources.

Increasingly, settings are choosing to allow older children to use popular search engines, such as: Google or Bing, rather than specific "child friendly" tools, as these are the tools children are most likely to use at home. Educational settings should be aware that, whilst tools such as Google and Bing will allow children to access a greater wealth of information, it also increases the risks of exposure to inappropriate content, so education and good classroom management will be vital.

Online searches provide an opportunity for children to develop critical thinking skills and explore the importance of evaluating, the reliability or bias of, internet content. This is particularly important for schools to consider in relation to their prevent duty, and when planning search activities on contentious or emotive topics; for example, researching the Holocaust online may lead to pupils access Holocaust denial sites and/or extreme right wing material- this should be carefully considered and risk assessed prior to the activity taking place.

How should educational settings authorise internet access?

Educational settings should provide internet access on the basis of educational need and should maintain a written record of who has onsite access and who has not.

Parents should always be made aware that their children will be granted internet access in school; this may be arranged annually, when children's home details are checked, or when children join the setting, as part of the Home-School/Setting agreement. It is not necessary to request parental consent for internet access, however if educational settings opt to do so, it is essential to record this data.

Children should not be prevented from accessing the internet at school, unless their parents have explicitly denied permission, or the child is subject to a specific sanction as part of the school behaviour policy. If parents deny internet access, the educational setting should discuss the implications of this on their child's education and try to explore the reasons why parents have requested this approach.

How can educational settings ensure they have appropriate filtering and monitoring in place?

KCSIE 2016 states that governing bodies and proprietors must '*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system*'. Educational settings are also required *'to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering'* in accordance with the statutory Prevent duties.

The UK Safer internet Centre has put together guidance for schools and colleges about appropriate filtering and monitoring.

What do educational settings need to consider when deciding 'appropriate' filtering and monitoring?

The UK Safer Internet Centre's guidance aims to enable governors, proprietors and leaders make informed decisions regarding what appropriate filtering and monitoring might look like within their setting.

The appropriateness of filters and monitoring approaches will depend on the age, abilities and specific vulnerabilities of learners; governing bodies and proprietors will also need to take into account, how often pupils access the IT systems, as well as any cost implications. What may be considered to be appropriate filtering and monitoring for one setting will be different for another; for example, approaches within a small rural early years setting/ primary school with limited IT equipment, are likely to be very different to that of a large urban secondary school with 1:1 devices.

Settings should undertake a robust risk assessment to explore proportionality of costs vs. risks; this will enable settings to evaluate the range of systems and/or providers available to them, and explore their potential benefits and limitations. Governing bodies and proprietors must ensure that the welfare of children is paramount at all time.

Educational settings that install or manage their own filtering systems may need to consider the responsibility and demand on management time; e.g. thousands of inappropriate sites are created each day and change URLs to confuse filtering systems. It is the leadership team's responsibility to ensure appropriate procedures are in place and all members of staff are suitably trained and supported to be able to supervise Internet access.

Kent settings who use the EIS School Broadband system will also have access to their LightSpeed system: this has a range of tools in place to adapt internet access according to the children's age, ability and maturity. Further information about LightSpeed can be accessed via the EiS Schools Broadband team.

Tablets

If educational settings use internet enabled devices, such as tablets, a robust risk assessment should be conducted by governors and proprietors, and clear risk management procedures implemented, in order to safeguard staff/ pupils and meet statutory obligations under KCSIE and Prevent. For example, devices which are not configured to require a "login", must have additional mechanisms in place to filter content and log access, such as; assigning children or staff a specifically labelled device, or logging and

reviewing which child or member of staff has accessed which device on a regular basis. These decisions and approaches should be recorded within the online safety policy.

Is 'appropriate filtering and monitoring' enough?

No. All members of staff and the wider community must acknowledge that filtering or monitoring solution cannot offer 100% protection from exposure to inappropriate or illegal content. An over-reliance on filtering and monitoring to safeguarding children online, could lead to complacency by staff and ultimately place children and staff, at risk of harm or allegations.

Governors, proprietors and leaders must be able to demonstrate a whole school safeguarding approach towards online safety.

How should educational settings respond to filtering breaches?

There should be a clear procedure to report and record breaches of filtering outlined in the Online safety policy, so all staff and pupils have a clear understanding of what to do and how to handle the situation. Consideration should also be given to how/.when parents, Internet Service Providers and specialist agencies (such as Kent Police or the Internet Watch Foundation) will also be informed.

For example:

- *Close or minimise the image or window immediately - don't try to navigate away.*
- *If children saw the content, talk to them about what has happened and reassure them.*
- *The content should be reported to the Internet Service and/or filtering provider*
- *The incident should be logged and recorded by the DSL.*
    - *Parents should be notified, if appropriate.*
    - *If content is thought to be illegal then it will be reported as appropriate to the Police and/or the Internet Watch Foundation*

What do educational settings need to consider about managing personal data online?

Educational settings will already have information about their obligations under General Data Protection Regulations (GDPR) and the Data Protection legislation; leaders should ensure that a relevant policy is in place. Statements within the online safety policy in relation to use of data are simply reminders of the need to protect data online; they will not be a replacement for a robust data protection or data security policy.

Information including a sample data protection policy (including guidance regarding encryption, secure email, staff training) and procedures for subject access requests can be accessed on Kelsi.

For advice and guidance relating to information governance or a contravention of GDPR, contact Michelle Hunt: Information Governance Specialist, Kent County Council michelle.hunt@kent.gov.uk 03000 416286. Further information is also available from the Information Commissioner's Office..

Should an Online Safety policy include IT security?

Whilst it may be helpful to include key messages, such as password safety, IT security is a complex issue which cannot be dealt with adequately within an online safety policy. Additionally, the Online safety policy should be clearly defined as a safeguarding policy, not a technical or ICT policy.

Educational settings may wish to seek specialist advice from their IP providers and from organisations such as the NEN.

What do educational settings need to consider regarding publishing information on their own websites?

Schools are required to publish certain information online, outlined here – this means that they **must** have a website. Whilst other settings may not be required to have a website, they can be useful platforms to communicate with the community and wider audiences.

The publication of information should always be considered from a safety and security viewpoint; websites are widely available to the public, so sensitive information about the setting, staff, events and children should be restricted to other places, for example: in a newsletter, staff handbook or on a secure part of the website which requires authentication from visitors.

Maximising official websites for online safety

It is highly recommended that schools/settings use their official websites to support parents/carers and children in understanding more about online safety. Some suggestions to help schools and settings achieve this are:

- Ensure that the Click CEOP button is clearly visible on the website (ideally on the main home page as well as in safeguarding areas).
- Create a specific online safety section for parents with accurate and up-to-date information, signposting to other agencies for support within the home.
- Create a specific online safety section for children with accurate and up-to-date information and include reporting processes where appropriate.
- Provide links to other websites for support e.g. Internet Watch Foundation, Think U Know, NSPCC and ChildLine
- Highlight the setting's reporting mechanisms, including named members of staff and contact details.
- Include the online safety policy (updated within the past year) with links to supporting resources e.g. Acceptable Use Policies, consent forms etc.
- Highlighting online safety within other areas of the website e.g. safeguarding, anti-bullying, behaviour, school newsletters etc.
- Include a clear outline of the schools approach to online safeguarding and should list a named contact person (e.g. the DSL) for parents and carers, staff and children.
- Ensure that content is: appropriate; not scaremongering; adapted to the needs of the community; and up-to-date.

For some settings, especially early years providers, an online presence may take place through social media channels rather than via formal website. Settings should access the use of social media guidance available on Kelsi to ensure that this is done safely and responsibly.

What do educational settings need to consider with regards to using cameras and publishing images and videos online?

Still and moving images and sound add liveliness and interest to a publication, display or website, particularly when children can be included. Nevertheless the security of staff and children is paramount.

Although common in newspapers, publishing children's names with their images is not acceptable by educational settings and images of a child must not be published without the parent/carer's written permission.

Please access the Kent template image use policy and guidance, "The use of cameras and images within education settings" for full information regarding the legal and safeguarding requirements for education settings.

What do educational settings need to consider with regards to managing email?

Email is an essential method of communication for educational settings, however, the implications need to be carefully considered and appropriate safety measures should be put in place.

Email can provide opportunities for unregulated contact from unknown individuals outside of the community. Spam, phishing and virus attachments can make email dangerous. Additionally if educational settings delegate access and therefore responsibility for email communication to users (including children and staff) there is a risk that inappropriate conduct or content could be shared. Setting provided emails should not be considered private, as most educational settings reserve the right to monitor official email communication; however a balance needs to be achieved between necessary monitoring to maintain the safety of the community and the preservation of employees human rights, both of which are covered by recent legislation.

Educational settings should carry out a risk assessment, from both a safeguarding and technical perspective, before using external email providers (such as, Google Apps for education) to provide staff and children with email systems; also, pay close attention to the sites terms and conditions- some providers have restrictions of use and age limits for their services.

Children's Use of Email

Educational settings need to consider and manage children use of setting provided email addresses.

The use of email identities, such as ***john.smith@school.kent.sch.uk,*** may not be appropriate for pupils, as it reveals personal information that could potentially put a child at risk.

Educational settings should also consider whether it is appropriate for children to have access to email addresses which allow them to communicate externally. For example, secondary schools and colleges may only allow pupils to communicate externally using email accounts which are monitored by the school, whereas primary schools and early years settings may find it more appropriate to use a whole-class email address which is managed by a member of staff.

Staff use of Email

Educational settings must ensure that they abide by data protection legislation and are conscious of where information is physically and/or virtually stored and how it may be accessed; email and data storage systems should be appropriately risk assessed and identified within relevant policies.

Professionals should ensure that their use of email at work complies with data protection legislation and confidential, sensitive or personal data is not sent electronically, unless it is appropriately encrypted or sent through a secure email system; simply password protecting file attachments may not be sufficient to meet breach data protection requirements.

The following links may be helpful for leaders to access:

- Kelsi: How to prevent being the next headline
- Kelsi: Child Protection Newsletter September 2014
- Access to Information

Educational settings need to consider whether school email can/should be accessed by members of staff when they are not on site (e.g. through personal devices) and how this should be managed in relation to confidentiality and data protection; this will need be covered elsewhere within policies (such as the AUP)

As well as protecting data, leaders should also ensure that members of staff develop an appropriate work life balance; staff should be discouraged from emailing children or parents late at night (unless in emergency circumstances or those agreed by the DSL) to promote appropriate professional boundaries.

Excessive out of hour use, such as late-night emails or during holiday periods, may place staff under unnecessary pressure to feel that they need to be available 24/7, which may ultimately impact on their well-being within the setting; this also applies to leadership and management.

What do educational settings need to consider with regards to managing educational use of videoconferencing and webcams?

Videoconferencing enables users to interact in ‘real time’, between different locations; equipment ranges from small PC devices (web cams) to large room-based systems that can be used for whole classes or lectures.

Videoconferencing introduces exciting dimensions for educational contexts; webcams are increasingly inexpensive and, with faster internet access, enable video to be exchanged and allow children to explore and source new experiences. The availability of live video can sometimes increase safety — you may believe that you can see who you are talking to — but if inappropriately used; a video link could reveal security details, place staff at risk or be used to exploit and abuse children.

Further information about use of images and cameras is available via the Kent template image use policy and guidance, “The use of cameras and images within education settings". Educational settings may choose to integrate this within their online safety policy.

What do educational settings need to consider with regards to managing learning platforms?

An effective learning platform or environment can offer a wide range of benefits to staff, children and parents, as well as support for management and administration. It can enable children and staff to collaborate in and across the setting, sharing resources and tools for a range of topics. It also enables the creation and management of digital content; pupils can develop online and secure e-portfolios to showcase examples of work.

As usage of the Learning Platform grows, issues may arise regarding content, inappropriate use and user's behaviour online; this must be carefully monitored by the leadership team who should review and update policy, practice and training, in order to minimise issues and concerns.

What do educational settings need to consider with regards to managing applications (apps) used to record, track or share children's progress?

In recent years, a number of apps for mobile devices have been launched which are specifically targeted at educational settings, allowing staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. These tools can provide considerable benefits, including improved engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before use.

Data Protection

Leaders and managers are ultimately responsible for the security of data and images, so they must have a clear understanding of where and how data will be stored, before purchasing or using any app, including who has access to it and any safeguarding implications. Educational settings will need to update parental consent forms relating to image use and data collection or may wish to have a separate form to include this use.

It also might be helpful for leaders to carry at a Data Protection Privacy Impact Assessment (DPIA), to help identify and reduce any privacy risks. The ICO website has a Code of Practice on DPIAs.

Safe Use

Users who have access to the app must be provided with clear boundaries regarding safe and appropriate use. Educational settings may wish to implement a specific AUP for all members of the community using the system or adapt the existing policy; the AUP should include: requesting that users log out of any accounts following use, use strong passwords, and requesting that users do not copy and share any images from the system.

Social Media

Why should educational settings cover social media within their policies?

Educational settings must acknowledge that social media is an everyday part of life and can offer exiting learning and communication opportunities; however it also brings a variety of risks.

- Social Media tools allow individuals to publish unmediated content.
- Social media tools can connect people with friends and family members but also with strangers – both known and unknown contacts can bring benefits as well as risks.
- Users can be invited to view personal spaces or content and leave comments, over which there may be limited control.

Examples of social media includes: blogs, wikis, social networking, forums, bulletin boards, multiplayer online games, video/photo sharing, chatrooms, instant messenger and many others. . Naming specific sites within a social media policy should be avoided, unless it is the setting's official social media channel, as popular sites are constantly changing and may cause misinterpretation.

Clear guidance will be required to ensure that:

- Educational settings are not exposed to legal risks;
- The reputation of the setting is not adversely affected;
- Users are able to clearly distinguish whether information provided via social media is legitimately representative of the setting;
- All members of the community are safeguarded from harm (both on and offline).

Can educational settings put guidance in place regarding staff personal use of social media?

Yes. KCSIE highlights that governing bodies and proprietors need to ensure that settings have a *"…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*."

Educational settings must provide appropriate guidance and boundaries to ensure that members of staff understand the setting's professional expectations, however this does not mean settings can ban members of staff from using social networking sites in their own personal time.

Educational settings can find guidance and supporting resources within the "Using Social Media in Educational Settings" and the "Acceptable Use Policies for Education Settings and their Wider Communities" documents available on the Kelsi website.

Reputational Management

All members of staff should be made aware of the potential risks of using social media; professionally and personally.

Safeguarding leads should encourage staff to carefully consider:

- The appropriateness of information and content they publish online and how this may reflect on their professional reputation or the reputation of the setting;
- Discussing online expectations with friends and colleagues (to ensure they don't post inappropriate content on their behalf);
- Securing their profiles (e.g. passwords) and ensuring their accounts and posts are set to private;
- The public and permanent nature of the internet- even with privacy settings, pictures and posts could be screenshotted or shared without their knowledge or consent.

DSLs may find following links helpful to share with staff:

- Childnet: For you as a professional
- Childnet: Professional reputation
- Safer Internet Centre: Professional reputation

Pupils and Parents as 'Friends'

Adding pupils and/or their family members as "friends" on personal social networking sites has been highlighted within several serious case reviews as a potential indicator of an unsafe culture. Unchallenged, this practice can blur professional boundaries between staff, families and children and can undermine the community's ability to identify and raise concerns about inappropriate professional conduct.

Leaders, managers and DSLs should ensure that there is a clear policy regarding staff contact with children and their family members outside of work; staff should ensure that communication is always transparent and open to scrutiny. We recommend that all members of staff be advised **not** to communicate with, or add as 'friends', any current or past pupils or their family members via personal social media sites, applications or profiles.
Many members of staff add pupils, or parents, as friends with good intentions, such as, offering additional support or keeping in touch through the next stages of their life. Although members of staff may feel that they can keep themselves safe, they could be putting themselves in a vulnerable position.

Likely risks for staff include:

- Sharing personal information or content which could be misinterpreted or shared publically without their knowledge or consent.
- Having access to personal information about families which could lead to safeguarding concerns; for example if pupils or parents post concerning content or material
- Undermining their professional reputation; ex pupils may have friends or other family members who are still within the community
- Allegations being made against them
- Being exposed to unwanted contact and/or harassment from members of the community and beyond

Ex-Pupils

There is no legal age or precedent whereby it becomes 'acceptable' for staff to add ex-pupils onto personal social networking sites.

Some educational settings have chosen to implement a recommended age/ time limit, before staff can add ex-pupils as friends; for example, when they are 18, or 2/3 years after they have left the school. Unfortunately, this approach creates 'grey areas', whereby professional boundaries can become blurred, leaving both staff and pupils (current and ex) in a vulnerable position; for example, a 6th form student who turns 18 before leaving the school or an ex-pupil who has younger siblings that still attend the school, who now have access to their personal social network.

The best approach is to promote a honest relationship between staff and the DSL, so online activities can be appropriately risk assessed and managed. For example, if ongoing contact with children or parents is required after they have left the setting, it may be agreed that staff can use their work email address or official social media channel, rather than personal social media accounts; this ensures that communication is transparent and open to scrutiny and will help safeguard staff from allegations.

Pre-Existing Relationships

There are certain circumstances where a pre-existing relationship between staff and current or ex-pupils and/or their family members, may compromise a member of staff's ability to comply with the policy, for example, if their own children/family members attend the setting, or they are long-term friends with the parent of a pupil. This must be disclosed to the DSL, Headteacher or manager to ensure the relationship is formally acknowledged, risk assessed and professional boundaries/conduct are agreed.

Can educational settings put guidance in place regarding children's use of social media?

Yes. Much like the expectations we put in place for children and young people with regards to their offline behaviour, educational settings should be clear about appropriate and responsible online behaviour too, which will include the use of social media.

Whilst many educational settings choose to block access to social media sites on school/setting equipment, it cannot be assumed that children will not access them offsite or when using personal devices. Children and young people should be given age appropriate education regarding safe and responsible use; this is likely to vary according to the age of the children and the possible safeguarding risks.

If specific concerns regarding children's use of social media are bought to the setting's attention, the DSL should ensure it is formally recorded, along with any action taken. In cases where children are using social media sites inappropriately (for example, cyberbullying, posting personal information, adding strangers as friends) or there are other safeguarding concerns due to vulnerabilities, the setting should respond in line with existing policies, such as: Anti-bullying, Child protection/Safeguarding or Behaviour policy.

Underage use of Social Media

Many popular social media services such as Facebook, Instagram, Twitter and YouTube have age restrictions of 13+. It is not a criminal offence for a child (or a parent) to lie about their age in order to set up an account, but education settings should be aware that the age limit is in place to protect children's privacy and to prevent them being targeted with unsuitable advertisements; due to the COPPA (Children's Online Privacy and Protection Act) legislation.

It is important for educational settings to recognise that, if we simply ban children from using social media and do not discuss safe behaviour, many of them will continue to use popular social media sites without advice or support, which could place them at increased risk of harm. Children may also be more likely to lie about or hide their online behaviour and may not feel able to disclose concerns if they fear being punished.

If educational settings are made aware of underage social media use, the DSL should speak directly to all children and parents involved in order to share their concerns and ensure that appropriate action is taken. In some cases, schools and settings could consider reporting accounts to social media sites for removal, however, leaders must be aware that this approach is unlikely resolve the problem as pupils may be able to create additional accounts; education for all members for the community about safe use of social media is therefore essential.

Should educational settings use social media officially?

Educational settings are encouraged to adopt a social media presence which works best for them.

Some educational settings decide not to have an official social media presence, but many are finding that this is no longer a choice; some settings find that a social media page has been automatically generated for them by the website, based on 'location tagging', or a member of the school/setting community has created an unofficial page or group to communicate and network, e.g. Parent Teacher Associations.

If educational settings are not actively engaged in developing or managing their social media presence, they may find it difficult to implement strategies to safeguard all members of the community or to respond effectively to issues if they occur. You cannot respond effectively to positive or negative content posted online if you don't know what is being posted!

Further guidance and considerations around this topic (including a checklist and sample risk assessment templates) can be found in the "Using Social Media in Educational Settings" document available on Kelsi.

Use of Personal Devices and Mobile Phones

Why do educational settings need a policy regarding use of personal devices and mobile phones?

Mobile technology and other personal devices, including: mobile phones, tablets, smart watches, fitness trackers, e-readers, electronic dictionaries, digital cameras and laptops are an everyday item in today's society; even children in early years settings may own and use personal devices regularly.

Educational settings must take steps to ensure that mobile technology is used responsibly and that the use of mobile phones and/or devices does not impede teaching, learning and behaviour.

The EYFS 2017 requires all early years childcare providers to have a clear safeguarding policy which *'covers the use of mobile phones and cameras in the setting'*, whilst KCSIE 2016 states that all schools and colleges must have *'a clear policy on the use of mobile technology'.* Policy regarding personal devices and mobile phones can be included within the online safety policy, embedded within other existing polices (such as Code of conduct) or kept separate.

What are some of the risks posed by personal devices and mobile phones?

Personal devices and mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged
- Their use can render children or staff subject to online (cyber)bullying
- Internet access on phones and personal devices can allow children and adults to bypass school monitoring and filtering systems
- They can undermine classroom discipline as they can be used on "silent" mode
- If used to access data, they can breach data protection and confidentially policies
- Mobile phones and devices with integrated cameras and other recording systems could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of children or staff

Devices which are not internet enabled still possess an element of risk which should be considered; taking and sharing indecent or inappropriate images can place children at risk of significant harm and can occur on any devices with inbuilt cameras.

Can educational settings ban children, staff and visitors from having personal devices and mobile phones?

Decisions regarding the use of personal devices and mobile phones will be down to leaders and managers; however a policy which totally prohibits children, staff or visitors from having mobile phones or personal devices when on site could be considered to be unreasonable and unrealistic. For example, many parents would be concerned if their child were not allowed to carry a mobile phone on journeys to and from school, and many staff use mobile phones to stay in touch with family.

Managers and leaders should implement a robust risk assessment to explore the benefits and risks, to ensure that a proportional and realistic policy decision is made; where possible, parents, children and staff should be included in the decision making process in order to increase engagement and develop whole school/setting ownership of the policy. Decisions should be supported with robust training and policies, which clearly identify the expectations for safe use as well as sanctions for misuse.

Educational settings that elect to allow members of the community to use their own devices for educational use within the classroom may wish to access the National Education Network (NEN) guidance.

How should educational setting's policies manage children's use of personal devices and mobile phones?

Children should be given explicit education regarding appropriate use of personal devices and mobile phones, in accordance with their age and ability.

Policies should identify the specific expectations regarding children and young people's safe use of mobile phones and personal devices. For example, *mobile phones and devices must be kept securely in a locker,* or *must be locked in a secure place in the school office at the start of the school day*. Within an early years settings it is significantly less likely that children will be bringing mobile phones onto the site, however they may bring other devices such as tablets, music players and games consoles.

Educational settings with residential provision, such as boarding schools or residential special schools, should consider how best to balance their safeguarding responsibilities with the need for children to take part in age appropriate, peer activities on the internet, such as: staying in touch with friends and family. Residential Schools and settings must ensure their policies explicitly cover how the school will monitor and regulate children's use of the internet, including via personal devices, out of school hours; parental consent should be considered, along with the views of the children.

Educational settings should ensure that their policies regarding confiscation, screening and searching are up-to-date and are clearly communicated to all members of the community, including pupils and parents. The Department for Education has guidance available for headteachers. The SWGfL has a template 'Search and Deletion Policy' which schools may wish to access and adapt.

Should educational setting's policies cover staff's use of personal devices and mobile phones?

Yes. Unsafe or inappropriate use of personal devices and mobile phones can place staff at risk of allegations and can undermine settings safeguarding culture.

Leaders and managers should ensure that the policy details the specific expectations regarding safe use of staff personal mobile phones and other personal devices. For example, *staff personal mobile phones and devices must be kept securely in a locker or locked draw*.

Leaders should be aware that seizing and searching members of staff's personal devices may be unlawful. If leaders feel this is required or appropriate, for example if a criminal offence may have been committed, then the appropriate agency should be informed. The DSL may wish to seek advice from the

Education Safeguarding team or the LADO (Local Authority Designated Officer) if there has been an allegation against a member of staff which may require seizing staff members' personal devices.

Should staff be allowed to use personal devices and mobile phones?

The use of personal devices and mobile phones by staff to take photos/videos of children is highlighted within the Image use guidance and should be read by leaders in conjunction with this document when making policy decisions.

Leaders and managers will need to consider possible risks which could arise as a result of allowing staff to use personal devices for official business, for example, automatically forwarding work emails to their personal devices; this may raise concerns regarding potential data protection and confidentiality breaches, for example, if a personal device is lost or stolen or shared with family members. Leaders and managers should identify expectations regarding appropriate and proportional use of personal devices to access work related content, including work email and take steps to ensure possible risks can be mitigated, for example, using authentication, password protected webmail clients and encryption, as well as appropriate training and staff induction.

How should educational settings manage visitors' use of personal devices and mobile phones?

Visitors will include a range of members of the community, such as: other professionals, volunteers, parents/carers, student placements and contracted or temporary staff. Many visitors will not have received any professional training with regards to online safety.

Leaders and managers must ensure that policies, regarding safe and appropriate use of personal devices and mobile phones, also apply to visitors, in order to minimise risks, such as:

- Using personal devices to take photos of a child and sharing them online
- Using personal devices to access inappropriate content
- Using personal devices to access illegal content
- Sharing confidential, sensitive or personal information

Decisions regarding visitors' use of personal devices and mobile phones should be clearly communicated; for example displaying signage and/or posters in visible areas such as entrance gates or reception. Some settings may choose to provide visitors with specific written expectations when they arrive on site, for example in the form of a specific AUP or a leaflet.

Members of the community, particularly staff and pupils, should be empowered to challenge visitors if they identify a breach of policy; for example if a member of staff observed a contractor carrying out site maintenance using their phone on the playground when children are present, they would be expected to ask the contractor to put the phone away and to report the situation to the DSL.

Responding to Online Incidents and Safeguarding Concerns

Online Safety incidents can occur unintentionally or deliberately by people acting inappropriately or even illegally. Online safety incidents can have an impact on children, members of staff and the wider community, both on and off site, and can have civil, legal and disciplinary consequences as well as raising child protection concerns.

Many online safety concerns can be managed at a personal level by ensuring members of the community are able to identify and report concerns. Members of staff are often the first line of defence; their observation of classroom behaviour is essential in recognising concerns about children and in developing trust so that issues are reported. Educational settings should ensure that all members of the community know how to respond if they encounter inappropriate content or behaviour online. Parents, staff and children should know how to use the settings complaints procedure.

DSLs should be familiar with the relevant Kent Safeguarding Children Board Threshold and procedures regarding online safety, including but not limited to:

- 2.2.2: Children Who Exhibit Harmful Behaviour including Sexual Harm (Assessing and Providing Interventions)
- 2.2.7: Working with Sexually Active Young People
- 2.2.9: Bullying
- 2.2.10: Online Safety, Child Abuse and Technology
- 2.2.11: Safeguarding Children Abused through Sexual Exploitation

Staff must be vigilant and challenge or report concerning behaviour by another member of staff (on and offline), in order to maintain a safe culture; concerns may vary from unintentionally inappropriate jokes, comments or actions to deliberate illegal activity. Allegations about staff conduct online should be manged in line with the settings allegations policies and procedures.

If a concern is reported to the setting, the facts will need to be established and evidence should be gathered where possible and safe or appropriate to do so. A minor transgression of the 'rules' can sometimes be dealt with by a member of staff, whereas other situations could potentially be serious and a range of sanctions may be required; this should be linked to the disciplinary/behaviour policy. Potential child protection issues must always be referred to a DSL. Incidents whereby police involvement may be required should be dealt with in line with Kent Police's Schools Incident Policy. Further advice on dealing with potentially illegal behaviour should be discussed with the Kent Police or the Education Safeguarding Team.

If the concern relates to inappropriate or illegal activity on school computer equipment, the level of response required should be proportionate to the offence disclosed; the decision to involve police should be made as soon as possible. If educational settings are unsure about how to respond to online safety concerns, they should consult with the Education Safeguarding Team.

Some settings may wish to cover responding to online safety incidents within the Child protection policy, rather than the online safety policy.

Should we alert parents or other settings about online safety concerns?

In some cases, settings may feel that it is necessary to warn parents about an online safety issue, or alert other local settings so they can cascade information within their community.

Headteachers, managers, proprietors and DSLs must ensure that the information being shared does not identify children, families and schools involved, or alert offenders to a live police investigation as this could result in children being placed at risk of harm and may prevent appropriate criminal action from being taken. Education settings should also be mindful not to share false or factually inaccurate rumours before thoroughly checking the source of the information.

If any Kent schools or settings have concerns about on or offline safeguarding issues which they feel need to be shared with parents urgently, or with other schools and settings, they should speak with the Education Safeguarding Team for advice and guidance.

Procedures for Responding to Specific Online Incidents or Concerns

The following content is provided to help education settings make appropriate safeguarding decisions when responding to specific online safety issues. This content is not exhaustive and cannot cover every eventually, so professional judgement and support from appropriate agencies such as the Education Safeguarding Team, Police, CSET and Children's Social Care is encouraged.

What is 'sexting'?

"Sexting" or Youth Produced Sexual Imagery can be defined as images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. These images may be shared between children and young people and/or adults via a mobile phone, webcam, handheld device or website.

Children typically do not use the term "sexting", usually referring to the images as "selfies" or "nudes". Children and young people will always look to push boundaries, especially when they go through puberty and/or are an age where they are more sexually and socially aware.

Youth Produced Sexual Imagery may be taken or shared by children or young people:

- Out of curiosity or naivety
- As a response to peer pressure or cyberbullying
- As part of sexual exploration or 'flirting'
- As part of a trusting relationship between peers
- impulsive behaviour
- exploitation or blackmail from a friend, partner, or other on or offline contact

Consequences of 'Sexting'

Having intimate photos forwarded to others or shared online can cause emotional and reputational damage, including isolation, bullying, low self-esteem, loss of control, creating of a negative "digital footprint" or online reputation, harassment, mental health difficulties, self-harm, suicide and increased risk of child sexual exploitation.

There can also be criminal consequences to sharing Youth Produced Sexual Imagery. Crimes involving indecent photographs (including pseudo images) of a person under 18 years of age, fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988;under this legislation, it is a crime to:

- Take or allow an indecent photograph to be taken;
- Make an indecent photograph (including downloading or opening an image that has been sent via email);
- Distribute or show an indecent image;
- Advertise indecent images;
- Possess an indecent image for personal use or with the intention of distribution.

This applies even if the images are sent or shared by someone under the age of 18, with consent. "Sexts" may be viewed as police evidence and it is essential that schools secure devices and seek advice immediately when dealing with concerns.

It should be noted that prosecution of children for sharing indecent images for a first offence is rare, as a conviction for such offences is likely to have long term implications for children's future health and wellbeing.

How should educational settings respond to 'sexting'?

According to KCSIE, all members of staff need to be aware of peer on peer abuse, including sexting; staff must be able to recognise and respond to sexting concerns.

It is essential that schools and settings handle 'sexting' incidents as carefully as possible and offer support to all parties involved. They will also need to abide by the law and not compromise police investigations; the decision to criminalise children and young people for sending sexualised images will need to be considered on a case by case basis based on a number of factors including age, intent and vulnerability of children involved.

Should an incident arise which necessitates criminal investigation, the phone/device, and any other devices involved or identified as potentially having access to the imagery, may need to be seized; schools and settings should ensure their policies regarding seizing and searching are robust and up-to-date.

- DSLs should access and consider the guidance as set out in UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.
- Specific advice for responding to youth produced sexual imagery for professionals working within Kent can be accessed via KSCB.
- Appendix 4 includes questions to help DSLs consider how best to respond to concerns relating to youth produced sexual imagery.

Educational settings will want to take as many preventative measures as they can to educate young people about the risks of 'sexting'. Early years and primary are an essential time to educate children about safe and responsible taking/ sharing of images, as this will them to develop resilience against potential peer and social pressure to take and share sexual imagery when they are older.

A range of appropriate educational resources for children and parents can be accessed in the UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'

What is Online Child Sexual Abuse and Exploitation (OCSAE)?

Online Child Sexual Abuse and Exploitation (OCSAE) within this policy context is specifically defined as when children are sexually abused or exploited through the use of technology and the internet; typically this may be considered "online grooming", however this term can be to be too narrow.

Online Child Sexual Abuse and Exploitation (OCSAE) can include:

- Deceiving or coercing children into producing indecent images of themselves
- Blackmailing children with youth produced sexual imagery
- Adults building a sexual relationship with children and young people
- Engaging children in sexualised chat
- Contact offending – meeting with children in real-life to abuse them
- Engaging children in sexual activity over webcam
- Peer on peer abuse
- Child Sexual Exploitation - Children and young people being:
    - Given technology by offenders in exchange for sexual acts
    - Tracked by offenders using mobile technology
    - Filmed or photographed naked or performing sexual acts

There can various criminal laws with regards to OCSAE. This includes (but is not limited to):

- The Sexual Offences Act 2003 – Section 15. Meeting a child following sexual grooming.
- The Sexual Offences Act 2003 – Section 8. Causing or inciting a child under 13 to engage in sexual activity
- The Sexual Offences Act 2003 – Section 10. Causing or inciting a child to engage in sexual activity.
- The Sexual Offences Act 2003 – Section 12. Causing a child to watch a sexual act
- The Sexual Offences Act 2003 – Section 13. Child sex offences (section 10, 11 and 12) but committed by children (offender is under 18).
- The Serious Crime Act 2015 - Part 5. Protection of Children - Section 67. Sending a child sexualised communications.

How should educational settings respond to OCSAE concerns?

Concerns regarding OCSAE should be responded to in line with offline sexual abuse and exploitation concerns. DSLs should ensure that they are familiar with the relevant Kent policies and procedures and that information is available in line with existing child protection procedures.

The Child Exploitation and Online Protection Command, or CEOP Command, is a command of the UK's National Crime Agency (NCA) and is tasked to work both nationally and internationally to protect children from harm online and offline. Settings may feel that it is appropriate to signpost children and

parents to the CEOP safety centre to report concerns; the CEOP report button enables children and parents to reports online sexual abuse or exploitation directly to CEOP's child protection advisers.

Members of staff should follow the settings child protection policy and procedures if they are made aware online abuse. If DSLs have already reported an online abuse concern to local statutory services, such as the Specialist Children's Services or the Police, then a separate report to CEOP will not be required. If settings are unsure of whether a report should be made to CEOP, contact the Education Safeguarding Team for advice.

Online child sexual abuse can also link in with Child Sexual Exploitation and DSLs should access local support:

- The KSCB CSE toolkit
- CSET Team and Operation Willow.

How should educational settings respond to concerns regarding Indecent Images of Children (IIOC)?

Educational settings must be aware of and understand the law regarding indecent images of children. Specifically (but not limited to):

- The Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18. The Civic Government (Scotland) Act, 1982 replicates this.
- The Sexual Offences Act 2003 (England and Wales) provides a defence for handling potentially criminal images and this is supported by a Memorandum of Understanding which provides guidance on what is and is not acceptable.

It is an offence to possess, distribute, show and make indecent images of children. Making of and distributing indecent images of children includes printing and viewing them on the internet, otherwise known as 'downloading'. More information about these offences can be found within appendix 5.

If the educational setting believes illegal activity may have occurred using school computer equipment, the level of response required should be proportionate to the offence disclosed; the decision to involve police should be made as soon as possible. If DSLs are unsure whether the incident is of a criminal nature, they should consult with the Education Safeguarding Team or Police.

In cases where a suspected indecent picture or photograph is discovered, settings should secure the device immediately, and should not forward, save or print the image; as soon as they are made aware that an image may be illegal, appropriate advice must be sought immediately. A person could be considered guilty of a criminal offence (making and distributing) if they print or forward the image, unless they have been given explicit direction from the Police.

Where it is determined that an offence has been committed and a police investigation is warranted, all measures to preserve evidence should be undertaken.

- All copies (including digital or printed copies) of indecent images of children will be seized.
- If an officer decides that equipment needs to be seized, then they will need to determine if the equipment is networked. If in doubt as to whether the server should be seized or not, officers

should seek advice from the Police Digital Forensic Unit, as seizure of the server will have a significant impact on settings.
- It is essential that settings are aware of this possibility and they should ensure that measures are in place to enable the computer network to continue functioning should this situation arise.

In all cases, a detailed statement may be obtained to assist those who investigate the offence. The following information should be included in the statement:

- The identity of any material witnesses
- The name of the Internet service provider (ISP) or mobile telephone service provider in the case of images received through a telephone
- If known, the web address, name of the app or website through which the image was found or received;
- Any passwords or other procedure required to gain access to the website
- If known, the identity of the person who sent the image
- Any details relating to those involved, such as email address or screen names
- The reason for any delay in reporting the incident to the police (to assist investigators).

How can educational setting respond to and prevent online extremism?

Schools and settings should be mindful of the specific responsibilities and requirements place upon them under the Prevent Duty. The statutory guidance summarises the requirements as undertaking risk assessment, working in partnership, staff training and IT policies.

Educational settings should have clear procedures in place for protecting children who are identified to be at risk of radicalisation; these procedures may be set out in existing safeguarding policies and it is not necessary for settings to have distinct policies on implementing the Prevent duty. The online safety policy can play an important role, as it will highlight actions the setting will take to ensure that children are safe from terrorist and extremist material when accessing the internet.

KCSIE requires governing bodies and proprietors to ensure that suitable filtering is in place which takes into account the needs of the community. When ensuring appropriate filtering is in place, settings should be mindful to act in accordance with the law, much like when ensuring the filtering blocks other forms of illegal content. It should also be noted that radicalisation and extremist views can be shared and accessed on variety of platforms, including user generated or social media sites such as Facebook and YouTube. The way in which monitoring of internet and network use is managed will be down to individual settings to decide and implement, taking into account the curriculum and also the needs and abilities of the community, including those may be considered at increased risk of exposure to extremist content, such as unaccompanied asylum seeking children.

Settings should not rely on filtering to prevent radicalisation, as children are likely to have access to a range of devices within the home which may not be filtered or monitored; education around safe use is therefore essential. Settings should ensure that online safety education highlights the risks of extremist content online, especially regarding the use and power of social media as a tool in radicalisation.

As with all safeguarding risks, members of staff should be alert to changes in behaviour which may indicate that individuals may be at risk or in need of specific help or protection.

For further advice and support regarding radicalisation and extremism, please access the guidance on Kelsi or contact Nick Wilkinson, Prevent and Channel Strategic Manager, Nick.Wilkinson@kent.gov.uk

Useful links regarding radicalisation and extremism

- DfE: www.educateagainsthate.com
- Report online hate and terrorism: www.gov.uk/report-terrorism:
- NCALT e-learning : http://course.ncalt.com/Channel_General_Awareness/01/index.htm
- 'Zak' training: https://www.kent.ac.uk/sspssr/ccp/game/zakindex.html
- National helpline: 020 7340 7264 Counter.extremism@education.gsi.gov.uk
- Kent Police www.kent.police.uk/advice/community_safety/terrorism/terrorism_prevent.html

What is cyberbullying?

Online or cyberbullying can be defined as the use of technology, particularly mobile phones and the internet to deliberately hurt or upset someone. Under the Children Act 1989 a bullying incident should be addressed as a child protection concern when there is 'reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm'. In many cases cyberbullying is also considered to be a form of peer on peer abuse.

Cyberbullying is becoming increasingly prevalent with the rapid advances of modern technology. As technology develops, bullying techniques evolve to exploit it; it is crucial that children, young people and adults, use their devices and the internet safely and positively and are aware of the consequences of misuse.

When children or adults are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if those around them do not understand online bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

Cyberbullying may not always be intentional and repeated in the same way that traditional offline bullying is. Repeated harassment online could include an initial concern which is then shared or endorsed by others such as by "liking", "sharing" or "commenting". People may not feel that they are bullying by doing this and single issue may become more serious. It is very important that all incidents of online abuse are addressed as early as possible to prevent escalation

How should educational settings respond to cyberbullying?

Online bullying which takes place outside school must still be investigated and acted on appropriately when reported to schools; cyberbullying should be viewed and treated the same as "real world" bullying. Education staff, parents and young people have to be constantly vigilant and work together to prevent this and tackle it wherever it appears. Section 89 of the Education and Inspections Act 2006 gives headteachers the power to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Even where safeguarding is not considered to be an issue, educational settings may need to draw on a range of external services to support the child (or adult) who is experiencing bullying, or to tackle any underlying issue which has contributed to a child (or adult) doing the bullying.

Reassure

The first response should be to support the target and reassure them that they have done the right thing by reporting the bullying. Staff should advise them how to deal with bullying appropriately for example how to block bullies or report the users. They should be instructed to keep evidence of cyberbullying by taking screen prints (including times, dates, names and locations if possible) or keeping messages. They should be made aware of the importance of not retaliating and ensure they know how to access support (such as in school or via places such as ChildLine) if required.

The setting should then use existing pastoral systems and procedures to support the child and should take action as identified in the anti-bullying policy. This may involve speaking with the child's parents/carers or supporting them to do so themselves.

Respond

If possible the setting should identify the bully, discuss the concern with them directly (with evidence where possible) and then take action and instigate sanctions in accordance with the relevant policies (for example anti-bullying and behaviour). This is likely to include speaking directly with their parents and carers and share the concerns and discuss appropriate sanctions or action to be taken moving forward.

The setting should also consider how to change the behaviour/attitude of the bully with the use of sanctions, education, restorative justice and support etc. as appropriate. The incident, including action taken, should be logged and recorded in the anti-bullying and/or safeguarding records.

Remove and Report

The setting should seek to take action to try and remove the content, and contact service providers/ Local Authority/Police where relevant. It should be noted that in most cases the quickest way to have content removed is for the person who posted it to remove it, as some service providers will only remove content which breaches the sites terms and conditions.

Cyberbullying in itself may not always be a criminal offence, further information on legislation can be found in appendix 5. If an offence is suspected, the setting should seek assistance from the police in line with the schools incident policy and/or via 101. If it is an emergency, for example if someone is injured, or there is a risk to someone's life, then the setting should contact 999.

Re-evaluate

Following any cyberbullying concerns, settings should revisit their policies, procedures and educational approaches, to identify if alternative action could be taken or implemented to prevent future occurrences.

- Further advice and information on cyberbullying can be found on Kelsi
    - The Education Safeguarding Team has produced a template Anti-Bullying policy which includes cyberbullying.
- DfE: "Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies"
- Childnet have produced a range of resources and guidance that can be used to give practical advice and guidance on cyberbullying
- Specific advice is available on Kelsi for leaders and managers regarding responding to online bullying or complaints made on social media by parents and carers.

What is 'online hate'?

The police and the Crown Prosecution Service (CPS) have agreed the following definition for identifying and flagging hate crimes:

"*Any criminal offence which is perceived by the victim or any other person, to be motivated by hostility or prejudice, based on a person's disability or perceived disability; race or perceived race; or religion or perceived religion; or sexual orientation or perceived sexual orientation or a person who is transgender or perceived to be transgender*."

A hate crime can include verbal abuse, intimidation, threats, harassment, assault and bullying, as well as damage to property. The perpetrator can also be a friend, carer or acquaintance who exploits their relationship with the victim for financial gain or other criminal purpose.

Educational settings should be aware that, whilst there is likely to be a lot of content on the internet which may be considered to be offensive, much of it may not be illegal. UK laws have been written to ensure that people can speak and write (even offensive material) without being prosecuted for their views; however there are some situations whereby posting offensive content online may be viewed as illegal, either as harassment or as a hate crime.

How should educational settings respond to 'online hate' concerns?

In August 2017, the CPS published updated guidance regarding hate crime; they believe that online hate crimes should be responded to with the same robust and proactive approach used with offline offending. Therefore, schools should deal with incidents of online have in accordance with their Anti-bullying and Behaviour policies.

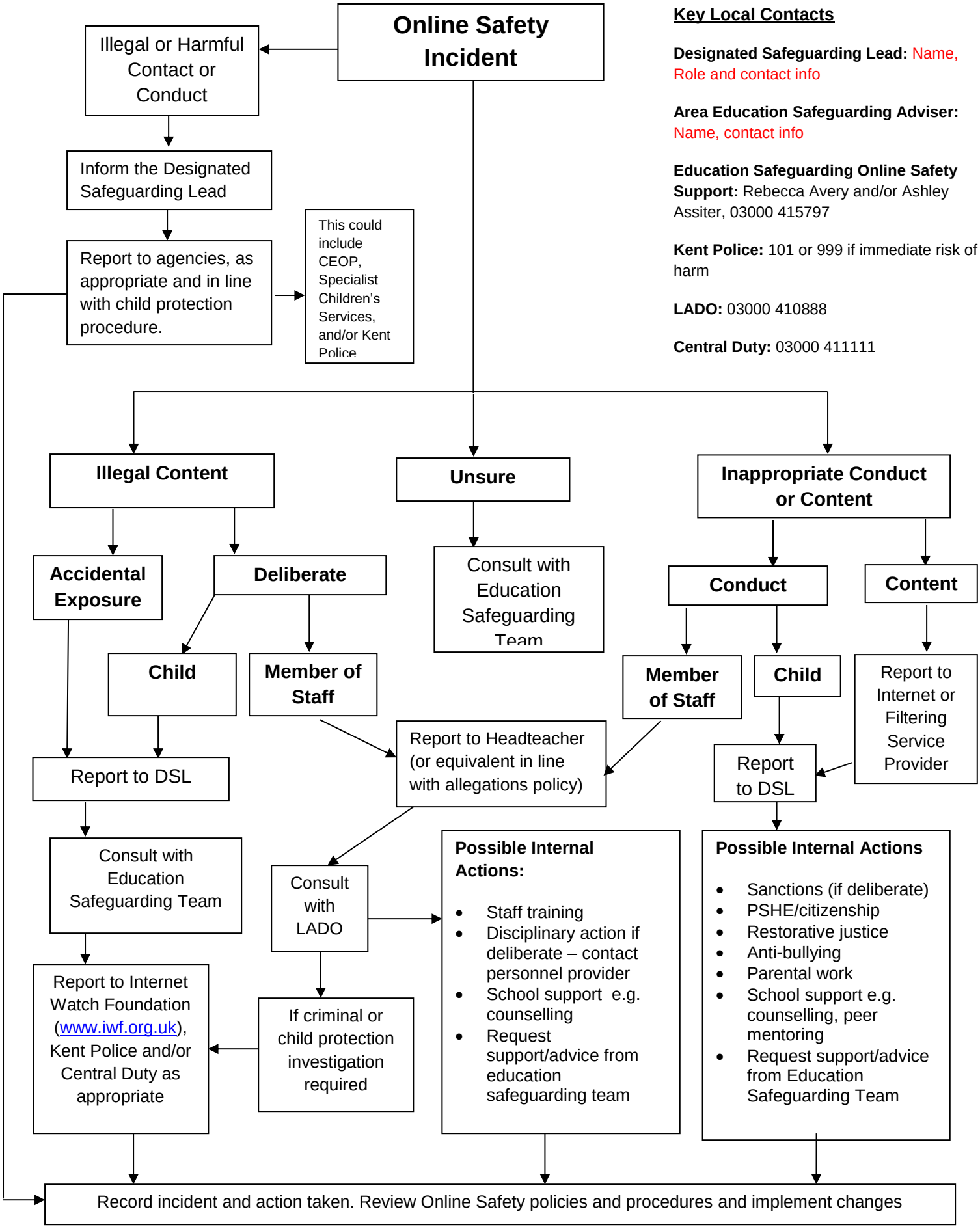
The CPS guidance also identifies that, in some circumstances, where online hate is perpetrated by children who may not appreciate the potential harm and seriousness of their actions, criminal prosecutions may not be appropriate.

Educational settings must ensure that they respond appropriately regarding online hate and discrimination, regardless of whether criminal action will be taken, and should support members of the community who may be targeted online.

Useful links

- www.report-it.org.uk – Report hate crimes
- www.stoponlineabuse.org.uk - Report online sexism, homophobia, biphobia and transphobia
- www.homeoffice.gov.uk/crime-victims/reducing-crime/hate-crime/
- www.stophateuk.org
- www.voiceuk.org.uk
- www.victimsupport.org.uk
- www.stonewall.org.uk

Appendix 1: Responding to an Online Safety Concern



Key Local Contacts

Designated Safeguarding Lead: Name, Role and contact info

Area Education Safeguarding Adviser: Name, contact info

Education Safeguarding Online Safety Support: Rebecca Avery and/or Ashley Assiter, 03000 415797

Kent Police: 101 or 999 if immediate risk of harm

LADO: 03000 410888

Central Duty: 03000 411111

Appendix 2: Online Safety Practice Recommendations for Education Settings

Policies and Practice

- Online Safety must not be viewed simply as an ICT Issue - it is a safeguarding issue for all staff to be aware of as safeguarding is everyone's responsibility.
    - Settings should be aiming to *"Protect them whilst they are in our care and educate them for when they are not".*
- The settings safeguarding approaches need to consider a range of online safety concerns inducing (but not limited to) child sexual exploitation, peer on peer abuse, including cyberbullying and sexting and radicalisation.
- Leaders and managers must have strategic oversight and awareness of online safety practice and issues within the setting.
- Settings should have an online safety policy. Stakeholder (including children, parents and staff) should be involved in the development and implementation of the online safety policy to help develop awareness and ownership.
- The Designated Safeguarding Lead (DSL) should take overall responsibility for online safety, with the support of other appropriate staff, for example with a group/committee.
- Settings should consider and be aware of external issues that could be brought on site e.g. online bullying, sexting etc. and should have appropriate policies and procures in place to respond to these issues.
- Settings should ensure there are Acceptable Use Policies in place for staff and pupils
    - Settings should consider adding a section in the Home School/setting agreement to encourage safe and appropriate behaviour by all members of the community.
- There should be support in place for staff and children when dealing with an online safety concern, including a clear reporting procedure.

Infrastructure and Technology

- Settings should take all reasonable precautions to ensure that online access is safe and secure, including appropriate supervision, risk assessments and implementing filtering and monitoring as appropriate to their community's needs.
    - The advent of 3G/4G and 'mobile internet' on devices means that filters etc. can be bypassed so filtering cannot be relied upon alone.
- Settings MUST consider data security and their statutory obligations – storage, transport, encryption etc. and have a policy around use of images (including obtaining parental consent for images to be used).
    - Access the Information Governance content for advice and support regarding data protection and information governance.
- Children and staff should be made aware of appropriate steps to take to ensure the safety and security of setting systems e.g. passwords (for all but the youngest of users), screen locks etc.

Education and Training

- All staff (whether paid or voluntary) should receive up-to-date and appropriate Online Safety training – either separately or as part of Child Protection/Safeguarding training on a regular (annual) basis
    - Training should give clear guidance to staff regarding safe and appropriate behaviour and communication.

- All members of staff need to be engaged in delivering an embedded and progressive online safety curriculum to empower children to build online resilience:
    - Byron Review (2008): *"…in a good school, all staff will have a role with regard to e-Safety, whether that be a teaching assistant or classroom teacher in a supervisory/awareness role, the ICT coordinator as the e-Safety coordinator, or school leaders who will have an awareness of the need for e-Safety at a strategic level. e-Safety and media literacy should be embedded across teaching and learning, not "bolted on".*
        - Settings who "do e-Safety" as a one of events or lessons are not fulfilling their requirements. Online safety should be taught across the curriculum and embedded across all subjects.
    - Online safety education should be ongoing throughout the curriculum from the moment children begin to use technology e.g. early years and cannot be taught as a one off lesson or assembly or in isolation.
    - Online safety education must take into account the different needs and abilities of all members of the school community and differentiate accordingly - a 'one size fits all' approach is unlikely to be successful with the most vulnerable and at risk students.
- Online safety education should involve and engage with the home so parents and carers should be involved with the policy development. Settings should engage with parents through a variety of opportunities to ensure online safety messages are consistent.
    - Additional information regarding can be found on Kelsi here

Standards and Inspection

- The Governing Body and/or Proprietor should be aware and engaged with the online safety agenda and ideally a Governor or Board/Trust member (as appropriate) should have lead responsibility for online safety.
    - The Governors/Trust role as a 'critical friend' is crucial to ensuring that settings are able to manage risk effectively in this area.
- All settings should record online safety concerns as part of their safeguarding records and systems which can be used to inform and shape policies and practice.
- Settings should monitor and audit their online safety work regularly and strive to achieve outstanding online safety practice.

Appendix 3: 'Child friendly' policy suggestions

Key points that settings could discuss and include in a child friendly policy are:

- What is 'Online Safety'
- Why our school/setting has an online safety policy
- What our school/setting does to keep us safe
- What our school/setting does to respond to online safety issues
- Acceptable use expectations
    - Including social media, phones and personal devices
- What to do if people are unkind
    - What should I do?
    - What should I not do?
- How pupils can get help if they are worried or upset online

Appendix 4: Questions to support DSLs responding to youth produced sexual imagery concerns

DSLs should follow the guidance available locally by KSCB and nationally via UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.

The following statements are provided to may help DSLs consider how best to respond to concerns relating to youth produced sexual imagery.

Child/Young person involved

- What is the age of the child(ren) involved?
    - If under 13, a consultation/referral to Specialist Children's Services should be considered.
    - If an adult (over 18) is involved, police involvement will be required. Contact 101 or 999 if there is risk of immediate harm.
- Is the child able to understand the implications of taking/sharing sexual imagery?
- Is the setting or any other agencies aware of any vulnerability for the children(s) involved such as special education needs, emotional needs, children in care, youth offending?
- Are there any other risks or concerns known by the school or other agencies which may influence decisions or judgements about the safety and wellbeing of the child(ren) involved such as family situation, children at risk of sexual exploitation?
- Has the child(ren) involved been considered under KSCB 2.2.2 "children who display harmful behaviours" or the KSCB CSE toolkit?

Context

- Is there any contextual information to help inform decision making?
    - Is there indication of coercion, threats or blackmail?
    - What was the intent for taking/sharing the imagery? For example, was it a "joke" or are the children involved in a "relationship"?
        - If so is the relationship age appropriate?
            - For primary schools a referral to social care regarding under age sexual activity is likely to be required.
    - Is this behaviour age appropriate experimentation, natural curiosity or is it possible exploitation?
- How was the setting made aware of the concern?
    - Did a child disclose about receiving, sending or sharing imagery themselves or was the concern raised by another child or member of the community?
        - If so then how will the setting safeguard the child concerned given that this is likely to be distressing to discuss.
- Are there other children/pupils involved?
    - If so, who are they and are there any safeguarding concerns for them?
    - What are their views/perceptions on the issue?
- What apps, services or devices are involved (if appropriate)?

The Imagery

Note: Schools and settings must NOT print/copy etc. imagery suspected to be indecent – devices should be secured until advice can be obtained

- What does the school know about the imagery?
- **Note: It is unlikely to be necessary for staff to view the imagery – access UKCCIS guidance**
    - Is the imagery potentially indecent (illegal) or is it "inappropriate"?
    - Does it contain nudity or sexual acts?
- Is the imagery on a setting device or a personal device?
- Is the device secured?
- Does the child(ren) know who has accessed the imagery?
    - Was it sent to a known peer, such as boyfriend or girlfriend, or an unknown adult?
- How widely has the imagery been shared? For example sent to one other child privately, shared online publically or sent to an unknown number of children/adults?

Action

- Does the child need immediate support and or protection?
    - What is the specific impact on the child?
    - What can the school put in place to support them?
- Is the imagery available online?
    - If so, have appropriate reports been made to service providers?
- Are other settings involved?
    - Does the relevant Designated Safeguarding Lead need to be identified and contacted?
- Is this a first incident or has the child(ren) been involved in youth produced sexual imagery concerns before?
    - If so, what action was taken? **Note: repeated issues will increase concerns for offending behaviour and vulnerability therefore an appropriate referral will be required.**
- Are the child protection and safeguarding policies and practices being followed?
    - Is a member of the child protection team on hand and is their advice and support available?
- How will the school inform parents?
    - With older children it is likely that DSLs will work with the young person to support them to inform parents
- Can the setting manage this issue internally or are other agencies required?
    - Issues concerning adults, coercion or blackmail, violent/extreme imagery, repeated concerns, vulnerable children or risk of significant harm will always need involvement with other agencies.

Appendix 5: Notes on the Legal Framework

Many young people and indeed some staff and adults use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

- This section is designed to inform leaders, managers and DSLs of potential legal issues relevant to the use of electronic communications.
- Language used within this appendix may be considered to be disturbing, traumatic or triggering for members of the community so it must be used sensitively and with caution.
- Legislation is constantly updating due to the rapidly changing nature of the internet and this list is not exhaustive.

This guidance must not replace professional advice and settings should always consult with their Area Safeguarding Adviser or the Education Safeguarding Adviser (Online Protection) from the Education Safeguarding Team, Legal representation, Local Authority Designated Officer or Kent Police if they are concerned that an offence may have been committed.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a "higher law" which affects all other laws. Within an education context, human rights for educational settings to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. Educational settings are obliged to respect these rights and freedoms, balancing them against rights, duties and obligations, which may arise from other relevant legislation.

Data Protection and Computer Misuse

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film, video and programs all qualify for

copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation.

Data Protection Act 1998 – be aware that this is subject to challenge following the Data Protection Bill 2017

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, organisations have to follow a number of set procedures.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Guidance for educational settings from the Information Commissioners Officer can be accessed at: www.ico.org.uk/for-organisations/education/

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

The Protection of Freedoms Act 2012

This act requires schools to seek permission from a parent / carer to use Biometric systems.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Obscene and Offensive Content; including Hate and Harassment

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence and this includes electronic transmission. For the purposes of the Act an article is deemed to be obscene if its effect is to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the content. This offence can result in imprisonment for up to 5 years.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This offence can result in imprisonment for up to 2 years.

Protection from Harassment Act 1997

This Act is relevant for incidents that have happened repeatedly (i.e. on more than two occasions). The Protection from Harassment Act 1997 makes it a criminal and civil offence to pursue a course of conduct which causes alarm and distress, which includes the publication of words, which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The victim can also bring a civil claim for damages and an injunction against the abuser, although in reality this is a remedy that is only used by individuals with the financial means to litigate, and only possible if the abuser can be identified, which is not always straightforward.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

The Protection of Freedoms Act 2012 (2A and 4A) and Serious Crimes Act 2015 (section 76) - Stalking and Harassment

The Protection of Freedoms Act 2012 was updated in 2015 and two sections were added regarding online stalking and harassment, section 2A and 4A. Section 2A makes it offence for a perpetrator to pursue a course of conduct (2 or more incidents) described as "stalking behaviour" which amounts to harassment. Stalking behaviours include following, contacting/attempting to contact, publishing statements or material about the victim, monitoring the victim (including online), loitering in a public or private place, interfering with property, watching or spying.

The Serious Crime Act 2015 Section 76 created a new offence of controlling or coercive behaviour in intimate or familial relationships which will include online behaviour.

Criminal Justice and Courts Bill 2015 (section 33) - Revenge Pornography

Section 33 makes it an offence to share private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress, often referred to as "revenge porn". The offence applies both online and offline and to images which are shared electronically or in a more traditional way so includes the uploading of images on the internet, sharing by text and e-mail, or showing someone a physical or electronic image. This offence can result in imprisonment for up to 2 years.

Sending images of this kind may, depending on the circumstances, also be an offence under the Communications Act 2003 or the Malicious Communications Act 1988. Repeated behaviour may be an

offence under the Protection from Harassment Act 1997. This law and the term “revenge porn” only applies to images or videos of those aged 18 or over.

For more information access the Revenge Porn Helpline.

Further information is available via the CPS.

Libel and Privacy Law

These matters will be dealt with under civil rather than criminal law.

Libel is defined as 'defamation by written or printed words, pictures, or in any form other than by spoken words or gestures' and as such could the author could be held accountable under Defamation law which was created to protect individuals or organisations from unwarranted, mistaken or untruthful attacks on their reputation. Defamation is a civil “common law” tort in respect of which the Defamation Acts of 1952 and 1996 provide certain defences. It applies to any published material that damages the reputation of an individual or an organisation, and it includes material published on the internet.

A civil action for defamation can be brought by an individual or a company, but not by a public authority. Where defamatory material is posted on a website, the person affected can inform the host of its contents and ask the host to remove it. Once the host knows that the material is there and that it may be defamatory, it can no longer rely on the defence of innocent dissemination in the Defamation Act 1996. This means that the person affected could (if the material has been published in the jurisdiction, i.e. in England and Wales) obtain a court order (an injunction) to require removal of the material, and could sue either the host or the person who posted the material for defamation.

If social media is used to publish private and confidential information (for example breaches of data protection act) about an individual, then this could give rise to a potential privacy claim and it is possible for individuals to seek an injunction and damages.

Education Law

Education and Inspections Act 2006

Section 89 of the states that every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents. This act (89.5) gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

The Education Act 2011

Section 13 makes it an offence to publish the name of a teacher who is subject to an allegation until such a time as that they are charged with an offence. All members of the community need to be aware of the importance of not publishing named allegations against teachers online as this can lead to prosecution. Schools should contact the LADO team for advice.

Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. This act gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. The DfE advice on these sections of the

Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"

The School Information Regulations 2012

This act requires schools to publish certain information on its website

Sexual Offences

Indecent Images of Children

Indecent images of children are images of children (under 18 years) depicting sexual posing, performing sexual acts on themselves or others, animals or sadomachisism. 'Indecent' is not defined in legislation but can include penetrative and non-penetrative sexual activity. A child for these purposes is considered to be anyone under the age of 18.

- under the **Protection of Children Act 1978** (as amended), the UK has a strict prohibition on the taking, making, circulation, and possession with a view to distribution of any indecent photograph or pseudo photograph of a child and such offences carry a maximum sentence of 10 years' imprisonment

- section 160 of the **Criminal Justice Act 1988** also makes the simple possession of indecent photographs or pseudo photographs of children an offence and carries a maximum sentence of 5 years imprisonment

These offences can include images taken by and distributed by the child themselves (often referred to as "Sexting"). Viewing an indecent image on a computer or phone means that you have made or are in possession of an image. Printing, forwarding, sharing and/or publishing can be considered to be distribution.

The Home Office has published guidance for young people to help them consider what is meant by the term "Indecent images of children".

Further information is available via CPS guide on indecent images of children

Possession of Prohibited Images of children

Section 62 of the Coroners and Justice Act 2009 ('the Act') created the offence of possession of a prohibited image of a child, punishable by up to three years' imprisonment.

In order for an image to be a "prohibited image", there are 3 elements that must be satisfied. An image must meet all 3 of the elements which are:

1. That the image is pornographic;
2. That the image is grossly offensive, disgusting, or otherwise of an obscene character; and
3. That the image focuses solely or principally on a child's genitals or anal region, or portrays a number of sexual acts

Further information is available via the CPS.

Sexual Offences Act 2003

There are many offences under the Sexual Offence Act 2003 which can be related to or involve the misuse of technology. This includes (but is not limited to) the following points.

- **Section 8. Causing or inciting a child under 13 to engage in sexual activity**
  - Can result in imprisonment for up to 14 years
  - *Examples – Asking, encouraging or succeeding to get a child to show intimate body parts, asking a child to perform a sexual act upon themselves. No lower age limit on offender.*
- **Section 9. Sexual Activity with a child**
  - Can result in imprisonment for up to 14 years
  - Any sexual intercourse with a child under the age of 13 commits the offence of rape.
- **Section 10 - Causing or inciting a child to engage in sexual activity**
  - Can result in imprisonment for up to 10 years
  - *Examples – Like S8 but child aged 13+ and offender aged 18+.*
- **Section 12 – Causing a child to watch a sexual act**
  - Can result in imprisonment for up to 10 years
  - *Examples – Masturbating over webcam, having sex with another over webcam, any sexual act a child can watch. Offender aged 18+.*
- **Section 11. Engaging in sexual activity in the presence of a child**
  - Can result in imprisonment for up to 14 years
- **Section 13 – Child sex offences committed by children**
  - Can result in imprisonment for up to 5 years
  - *Examples – Same acts as S10 and 12 but committed by children against children. Offender under 18*
- **Section 15 - Meeting a child following sexual grooming**
  - Can result in imprisonment for up to 10 years
  - The offence of grooming is committed if someone over 18 has communicated with a child under 16, at least twice (including by phone or using the Internet) and meets them or travels to meet with them anywhere in the world, with the intention of committing a sexual offence.
- **Section 16 - Abuse of position of trust: sexual activity with a child.**
  - Can result in imprisonment for up to 5 years
  - It is an offence for a person in a position of trust to engage in sexual activity with any person under 18 with whom they know as a result of being in their professional role. Typically, teachers, social workers, health professionals fall in this category of trust.
  - It is also an offence cause or incite a child with whom they are in a position of trust to engage in sexual activity, to engage in sexual activity in the presence of a child with whom they are in a position of trust, or cause a child with whom they are in a position of trust to watch a sexual act.

Criminal Justice and Immigration Act 2008

Section 63 makes it an offence to possess “extreme pornographic images”. 63 (6) identifies that such images must be considered to be “grossly offensive, disgusting or otherwise obscene”. Section 63 (7) includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”. Penalties for possession of extreme pornographic images can be up to 3 years imprisonment.

Further information is available via the CPS.

The Serious Crime Act 2015

Part 5 (Protection of Children) section 67 makes it a criminal offence for an adult (person aged over 18) to send a child (under 16) sexualised communications or sends communications intended to elicit a sexual communications. The offence is committed whether or not the child communicates with the adult. Penalties for sexual communication with a child can be up to 2 years imprisonment.

Section 69 makes it an offence to be in possession of paedophile manuals, information or guides (physically or electronically) which provide advice or guidance on sexually abusing children. Penalties for possession of such content can be up to 3 years imprisonment.

This law also removed references in existing legislation to terms such as child prostitution and child pornography and identified that this should be viewed to be child sexual exploitation.