Policy Document for: Online Safety

Approved: March 2020

Due for Review: March 2021

Contents

Introduction....4

Legislation and guidance....4

Roles and Responsibilities....4

Governors....4

Executive Principal....4

Heads of School....5

Designated Safeguarding Leads (DSL and DDSLs)....5

The IT Technician....5

All staff and volunteers....6

Teaching and class facing support staff....6

Parents....6

Visitors and members of the community....6

Pupils....7

Management of infrastructure....7

Educating pupils about online safety....7

SEND and Looked After Children....9

What is different for learners with SEND?....9

Online safety messages....9

Engaging parents and carers of SEND children....10

Informing policies and procedures....10

Useful Resources for parents/carers....10

Educating parents about online safety....11

Covid-19 – children learning at home....11

Cyber-bullying....11

Definition....11

Preventing and addressing cyber-bullying....11

Examining electronic devices....12
Sexting (Youth Produced Sexual Imagery)....12
What is 'Sexting'? 12
'Sexting' within the wider safeguarding context....13
Experimental 'Sexting' 13
Aggravated 'Sexting' 13
Risk Management....14
Acceptable use of the internet in school....14
Acceptable use of social media in and out of school for staff, parents and pupils....14
Staff and pupils using mobile devices in school 14
Staff using work devices outside school....14
How the school will respond to issues of misuse 14
Training....15
Using digital and video images 15
Data protection (GDPR) 15
Protocols for handling electronic communications....15
Unsuitable/inappropriate activities....16
Monitoring and reviewing 16
Appendix 1 – Online bullying....18
Appendix 2 - Acts of Parliament relevant to online safety in schools....19
Communications Act 2003 (section 127)....19
Computer Misuse Act 1990 (sections 1–3)....19
Copyright, Design and Patents Act 1988 19
Counter-Terrorism and Security Act 2015 (section 26)....19
Criminal Justice Act 2003....19
Criminal Justice and Immigration Act 2008 (section 63) 19
Data Protection Act 1998 (GDPR from May 2018) 19
Education and Inspections Act 2006 20
Malicious Communications Act 1988 (section 1) 20
Obscene Publications Act 1959 and 1964 20
Protection from Harassment Act 1997....20
Public Order Act 1986 (sections 17–29) 20
Racial and Religious Hatred Act 2006....20
Regulation of Investigatory Powers Act 2000 20
Sexual Offences Act 2003 20
Appendix 3 - Useful organisations/support services for reporting online safety issues....22
Grooming or other illegal behaviour 22
Criminal content online 22
Scams....22
Getting help/advice: for teachers....22

Getting help/advice: for professionals working with children 22
Appendix 4 – Responding to youth produced sexual imagery 23

Introduction

Our school community recognises the importance of treating online safety as an ever-present serious safeguarding issue. It is important to protect and educate both pupils and staff and have supportive mechanisms, policies and protocols in place to protect and support the school community.

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Head of Schools and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 , the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

Roles and Responsibilities

Governors

- Governors will ensure that appropriate filters and monitoring systems are in place on the school's IT resources.
- The governing board has overall responsibility for monitoring this policy and holding the Head of School to account for its implementation.
- The governing body will receive regular reporting on incidents of online safety and what actions have been taken to address them and support any person affected
- Governors will ensure that pupils are taught about online safety, for example through personal, social, health and economic education (PSHE) and through sex and relationship education (SRE).
- Governors are responsible for the approval of this policy and reviewing the effectiveness of the policy
- Agree and adhere to the Acceptable Use Policy for staff

Executive Principal

The Executive Principal is responsible for ensuring the online safety of members of the school community and will manage the education of pupils and training of staff in online safety and awareness of potential radicalisation in pupils.

The Education and Inspections Act 2006 empowers the Executive Principal, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, even though they may take place out of school, but are linked to membership of the school.

Heads of School

The Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Designated Safeguarding Leads (DSL and DDSLs)

Details of the school's DSLs and Deputy DSLs are set out in our **child protection and safeguarding policy** as well relevant job descriptions.

The Trust DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of School, IT technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Liaises with the local authority (LA) and reports to the Executive Principal any suspicions of pupils who may be becoming radicalised.
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of School so this can be shared with local Governing Body

This list is not intended to be exhaustive.

The IT Technician

The IT Technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Users may only access the school's networks through a properly enforced password protection policy.
- The Executive Principal is informed of any suspicions of pupils who may be becoming radicalised
- Ensuring that any online safety incidents are logged on CPOMS (through checking with the DSL team) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms of the Acceptable Use Policy and ensuring that pupils follow the **Acceptable Use Policy** for pupils
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Teaching and class facing support staff

Are responsible in particular for ensuring that:

- They report any suspected misuse or problem to the DSL/DDSL or Head of School for investigation, action and potential sanction.
- Digital communications with pupils (email/virtual learning environment should be on a professional level and only carried out using official school systems.
- Pupils understand and follow this policy and the pupil acceptable usage policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- They are aware of the online safety issues pertaining to email and social media usage and implement the school **social media, mobile phones and electronic devices policy**.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- They are alert to, and report to the Executive Principal, any suspicions of pupils who may be becoming radicalised.

Parents

Parents are expected to:

- Notify a member of staff or the Head of School of any concerns or queries regarding this policy
- Parents and carers will be responsible for endorsing (by signature) the pupil acceptable computer usage agreement.
- Ensure their child has read, understood and agreed to the Acceptable Use for pupils document

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, which is part of the Safeguarding leaflet held at reception, and expected to read and follow it. If appropriate, they will be expected to agree to the Acceptable Use Policy

Pupils

- Are responsible for using the school IT systems in accordance with the pupil acceptable usage policy and agreement, which they will be expected to sign before being given access to school systems.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials including suspicions of pupils who may be becoming radicalised, and know how to report such abuse.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices.
- Will be expected to know and understand school policies on the taking/use of images and on cyber-bullying.
- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Will understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school.

Management of infrastructure

The Trust will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The Trust will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School IT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the acceptable computer usage policy and any relevant LA online safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the IT technician and will be reviewed at least annually
- All users will be provided with a username and password by the IT technician.
- The administrator passwords for the school IT system, used by the IT technician (or other person) are also available to the Executive Principal or other nominated senior leader and kept in a secure place (eg school safe).
- Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by EIS.
- Any filtering issues should be reported immediately to the IT technician.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place in the acceptable computer usage policy regarding the downloading of executable files by users.
- An agreement is signed by members of staff in possession of school provided laptops regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- The school infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum: Although we are an Academy Trust, we follow the National Curriculum for Computing and Teaching online safety in schools https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

Online safety education will be provided in the following ways:

- A planned online safety programme will be provided as part of our Discovery curriculum in specific online safety lessons as well as wider curriculum such as PSHE– this will include both the use of IT and new technologies in school and outside school.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be helped to understand the need for the pupil acceptable computer usage agreement and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Pupils will be taught to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.
- Rules for use of IT systems/internet will be posted in all relevant rooms and displayed on log-on screens.
- Where pupils are allowed to search the internet freely, eg using search engines, staff are vigilant in monitoring the content of the websites the pupils visit.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- It is accepted that from time-to-time, for good educational reasons, pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT technician temporarily removes those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need.
- Pupils are taught in all lessons to be critically aware of the content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

From September 2020 **all** schools will teach: Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

SEND and Looked After Children

The Trust gives careful consideration to those children who may be particularly vulnerable online such as Looked After Children and those with Special Educational Needs and Disabilities (SEND). We use the support from Kent Local Authority to support our decision making processes on:

https://www.kelsi.org.uk/__data/assets/pdf_file/0011/74576/Online-Safety-for-SEND.pdf

What is different for learners with SEND?

The internet and technology are an integral part of everyday life for children. It is important that we acknowledge the positive opportunities the internet provides for young people with Special Educational Needs and Disabilities (SEND); the accessibility of images and video online make it an excellent learning tool, whilst global connectivity enables children with SEND to socialise and access support.

However, children with SEND are more likely than their peers to experience online issues such as cyberbullying, online grooming and exploitation. Similarly, children with SEND are more likely to have their internet use restricted and therefore have limited opportunities to learn through experience, develop resilience or seek support, which would empower them to use technology safely.

Online safety messages

For some learners, the use of abstract language and concepts can lead to confusion, frustration and misunderstandings. It is important that settings work together with their learners to build and develop a collaborative understanding of the terminology being used.

Online safety is a fundamental part of our safeguarding responsibilities and education settings should implement a range of targeted and differentiated strategies to enable learners with SEND to access the internet safely and appropriately. For example:

- What does the term 'online predator' mean to a child with SEND? Is it a dangerous person or a wild animal?
- Is an online contact still a stranger if you know their name or they send a 'friend request'?
- If you must never share personal information online, how do you tell online shops where to deliver your orders?

We are mindful that there are usually exceptions to rules which can sometimes be difficult for children with SEND to accept; ensure the 'rules' you provide are clear, consistent and not left open to interpretation. For example a learner who finds it difficult to understand abstract meaning may not be able to interpret hidden messages or metaphors in many popular video resources. We adapt our online safety messages such as instead of saying: "Don't share personal information online", consider a more realistic statement: "Always ask your trusted adult, before sharing personal information online".

Many learners with SEND will want to engage in the same activities as their peers, but may lack the understanding, skills or support to do so safely. Using the support of parents/carers, we implement a small step approach to online access, enabling learners to develop experiences and build resilience in the online environment.

Online safety education does not just take place within computing lessons but should form part of an embedded and progressive curriculum, including appropriate PSHE and Sex and Relationships Education (SRE).

One-off events or assemblies, provided by external visitors, cannot be as effective as directed, differentiated teaching which addresses the specific needs and vulnerabilities of your learners.

When teaching about online safety, learners with SEND may need:

- Complex online safety issues to be broken down and explained in greater detail
- To explore issues in a variety of contexts and approaches
- More examples of safe and unsafe practices
- Constant reinforcement and repetition of key safety messages
- Differentiated teaching resources and materials

Visual resources and verbal support can be useful for learners with SEND, but some learners may respond better to multi-media content such as videos, interactive presentations, screensavers or spoken/ sound recordings that they can associate with 'good' or 'bad' decisions. 'Know your friends with Josh and Sue' is an illustrated video from CEOP which uses clear facial expressions and visual clues to communicate basic online safety rules.

Some learners with SEND may intentionally test boundaries and contravene the rules in the Acceptable Use Policy (AUP) for pupils, which is given consideration in the writing of the policy. We also consider:

- Do all learners recognise and understand safe and unsafe behaviour online?
- Can they transfer rules about safety, or skills, from one activity and apply it to the online environment?
- Are there appropriate boundaries and support networks for learners at school?
- Are there appropriate boundaries and positive role models for learners at home?

Engaging parents and carers of SEND children

Parents/carers play a vital role in supporting their children learn how to be safe online, but may have their own concerns about insufficient computer skills or a limited understanding about the online environment can be off-putting for many parents, regardless of whether their child has SEND or not.

We reassure parents that online safety has more to do with parenting than technology; their child is likely to be vulnerable both on and offline, so we encourage parents to adopt similar mechanisms for supporting their child online, as they use in the 'real' world. For example:

- A parent assumes that their child is not physically or mentally capable of accessing the internet, so does not implementing blocks or filters.
- A parent is frightened that their child will be an easy target online, so bans internet access, restricting their child's ability to learn and develop online resilience.
- A parent assumes that their child, who is very technology literate, knows how keep themselves safe, so does not actively discuss online safety rules.

Both professionals and parents should take an active interest in children with SEND online activities and talk to them regularly about what they do online.

Informing policies and procedures

The SENCo is part of the DSL team and provides support when reviewing and updating policies so that the needs of our vulnerable children are considered in our procedures and practice. For examples, if we have a child with an EHCP who is particularly vulnerable online, this will be included in their EHCP targets. Similarly, we can use a Online Safety Plan with any child who demonstrates unsafe behaviour online, which is shared with the parents so they can support their child further at home.

We give consideration to the specific needs of our children to ensure they receive additional adult supervision where they may be unable to regulate their own online behaviour. Any child which requires additional supervision is tracked through our internal systems so that all staff are aware.

Vulnerable children may also find it difficult to explain or describe things that happened online; DSLs are aware of this when they investigate as some children may need to show what they did rather than tell.

Useful Resources for parents/carers

Parent Info: www.parentinfo.org/article/learning-disabilities-autism-and-internet-safety

Think U Know: www.thinkuknow.co.uk/parents/articles/Does-your-child-haveAutistic-Spectrum-Disorder/

Cerebra: www.cerebra.org.uk/help-and-information/guides-for-parents/learningdisabilities-autism-and-internet-safety-a-parents-guide/

The National Autistic Society: www.autism.org.uk/technology

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. We also take part in #WakeUpWednesday as part of the National Online Safety site www.nationalonlinesafety.com and share weekly updates and platform guides via email/school Facebook page with our parents.

This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head of School.

Covid-19 – children learning at home

During this unprecedented time, many children are accessing online learning and resources at home. In order to protect children as much as possible, we have shared information and a number of resources with parents.

Our website contains a separate Covid-19 tab. Within this there is a separate section for 'helping your child be safe online'. This encourages parents to share the Acceptable Use policy for children and talk through with them how to be safe and what to do if something makes them feel uncomfortable.

There are links to the Government released sites which support parents as well as online safety activities for the whole families.

Our safeguarding addendum sets out how online safety incidences will be recorded and investigated.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. We share the National Online Safety poster for online bullying with the children (see Appendix 1 on page 18).

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This will be covered in class as part of PSHE lessons (or during other curriculum time) and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. Resources can be found on National Online Safety to support best practice and address teacher workload.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school **behaviour policy**. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. For more information see the Trust policy on **Confiscation of inappropriate items**.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Sexting (Youth Produced Sexual Imagery)

KSCB Guidance for Professionals provides the following guidance to schools. Sexting is a safeguarding concern and taken very seriously by Timu Trust, as well as potentially being illegal.

What is 'Sexting'?

- Youth Produced Sexual Imagery (YPSI or "Sexting") 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/app.
- It is a crime to take, make, permit to take, distribute, show, possess, possess with intent to distribute, or to advertise indecent images of any person below the age of 18 (Crime and Justice Act 1988, section 160, Protection of Children Act, 1978, section 1,1,a).
- Professionals should be aware the prosecution or criminalisation of children for taking indecent images of themselves and sharing them should be avoided where possible. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children and young people especially if they are

convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.

‘Sexting’ within the wider safeguarding context

Sexting among children and young people is often considered to be commonplace within modern relationships. However it should raise professional concerns and in some cases may require further action or involvement with other agencies. “Sexting” can be defined as being “Experimental” or “Aggravated” (based on the Wolak and Finklehor model, 2011) and will require professionals to make informed judgements when responding.

Experimental ‘Sexting’

These incidents involve children or young people creating and sharing sexual images without additional concerns regarding criminal behaviour (beyond the creation or sending of images), without apparent malice towards others and involves the willing participation of those young people who were pictured. They can be classified in the following way:

- Romantic: Young people in ongoing relationships, make images for themselves or each other, and the images are not intended to be distributed beyond the pair. For example two 16 year olds are in relationship and are sharing sexual images which are not shared beyond their relationship.
- Sexual Attention Seeking: Cases in which images are made and sent between or amongst young people who were not known to be romantic partners, or where one young person takes pictures and sends them to many others or posts them online, presumably to draw sexual attention. For example a 13 year old shares a picture of their breasts to a 14 year old when “flirting” with them.
- Other: May include cases that do not appear to have aggravating elements but also do not fit into the Romantic or Attention Seeking sub-types. These involve either young people who take pictures of themselves for themselves (no evidence of any sending or sharing or intent to do so) or pre-adolescent children who did not appear to have sexual motives. For example an 11 year old taking pictures of their own genitals because they find it funny.

If children or young people engaging in experimental incidents are aged 12 or under, or are considered to be vulnerable then existing KSCB procedures should be considered, including (but not limited to) underage sexual activity, Child Sexual Exploitation toolkit and/or children who display harmful behaviour. The wider contextual information will also need to be considered.

Aggravated ‘Sexting’

These incidents involve additional criminal or abusive elements beyond the creation, sending or possession of sexual images. This may include the involvement of adults, for example soliciting sexual images from children and young people, or other illegal adult involvement. It may also involve criminal or abusive behaviour by minors such as sexual abuse, extortion, deception or threats; malicious conduct arising from interpersonal conflicts; or creation or sending of images without the knowledge or against the will of those who were pictured. They can be classified in the following way:

- Adult Involved. An adult (aged 18 or over) has developed a relationship with and/or coerced a child (17 or under) in criminal sex offences. The images are generally, but not always, solicited by the adult offender(s). For example a 16 year old girl is coerced into sharing sexual images of herself with a 25 year old man.

Aggravated cases are likely to need to be discussed with specialist children’s services and/or the police. Use of KSCB procedures for Child Sexual Exploitation, underage sexual activity and/or children who display harmful behaviour (HSB) may be required for referral to external agencies. Wider contextual information may also be asked for. This flowchart can be seen in Appendix 4 on page 23.

Risk Management

It is expected that all agencies will exercise professional judgement regarding responding to sexting. KSCB suggest that professionals use the harmful sexualised behaviour tool (www.KSCB.org.uk), Child Sexual Exploitation toolkit and threshold document to inform this decision making; however other agency or risk management tools may be appropriate. To support this professionals are recommended to discuss their concerns with their agency designated/named safeguarding lead. Kent Local Authority also recommend the use of https://www.gov.uk/government/publications/sexting-in-schools-and-colleges to support DSLs when making decisions.

NB: professionals must not print, forward, distribute or save any images or content believed to be an indecent image unless Police advice has been given.

Acceptable use of the internet in school

- All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the Acceptable Use Policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Acceptable use of social media in and out of school for staff, parents and pupils

See the **Social media, mobile phones and electronic devices** policy.

If social media is used for the purposes of online bullying, **Positive behaviour principles handbook** (Anti Bullying Policy) makes sanctions regarding bullying using new technologies very clear.

The school can take action against incidents that happen outside school if it:

- Could have repercussions for the orderly running of the school or
- Poses a threat to another pupil or member of the public or
- Could adversely affect the reputation of the school.

Use of social networking sites to harass, bully or intimidate would be covered by this irrespective of when/where the post was made.

Staff and pupils using mobile devices in school

See the **Social media, mobile phones and electronic devices** policy.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

See the **Staff Acceptable Use Policy** for full details.

- If staff have any concerns over the security of their device, they must seek advice from the IT Technician.
- Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on [behaviour and ICT and internet acceptable use – adapt according to what policies you have]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures/staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required e.g. through online CPD (as part of National Online Safety), newsletters and blog links
- The DSL team will all undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Using digital and video images

- When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Written permission from parents or carers will be obtained.

Data protection (GDPR)

From May 2018 personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations

Staff will ensure that they comply with the secure data handling guidelines by:

- Taking care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Using personal data only on secure password protected computers and other devices, and ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.
- Transferring data using encryption and secure password protected devices.

See the **Data Protection policy** for full details.

Protocols for handling electronic communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.

- Users will be expected to know and understand school policies on email, social media, mobile phones and other electronic devices
- Users must immediately report, to the Trust DSL, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content.

Unsuitable/inappropriate activities

Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on child protection, safeguarding and online safety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity eg:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Potential radicalisation of pupils.

Should any serious online safety incidents take place, the appropriate external authorities will be informed (eg local area designated safeguarding officer, police etc).

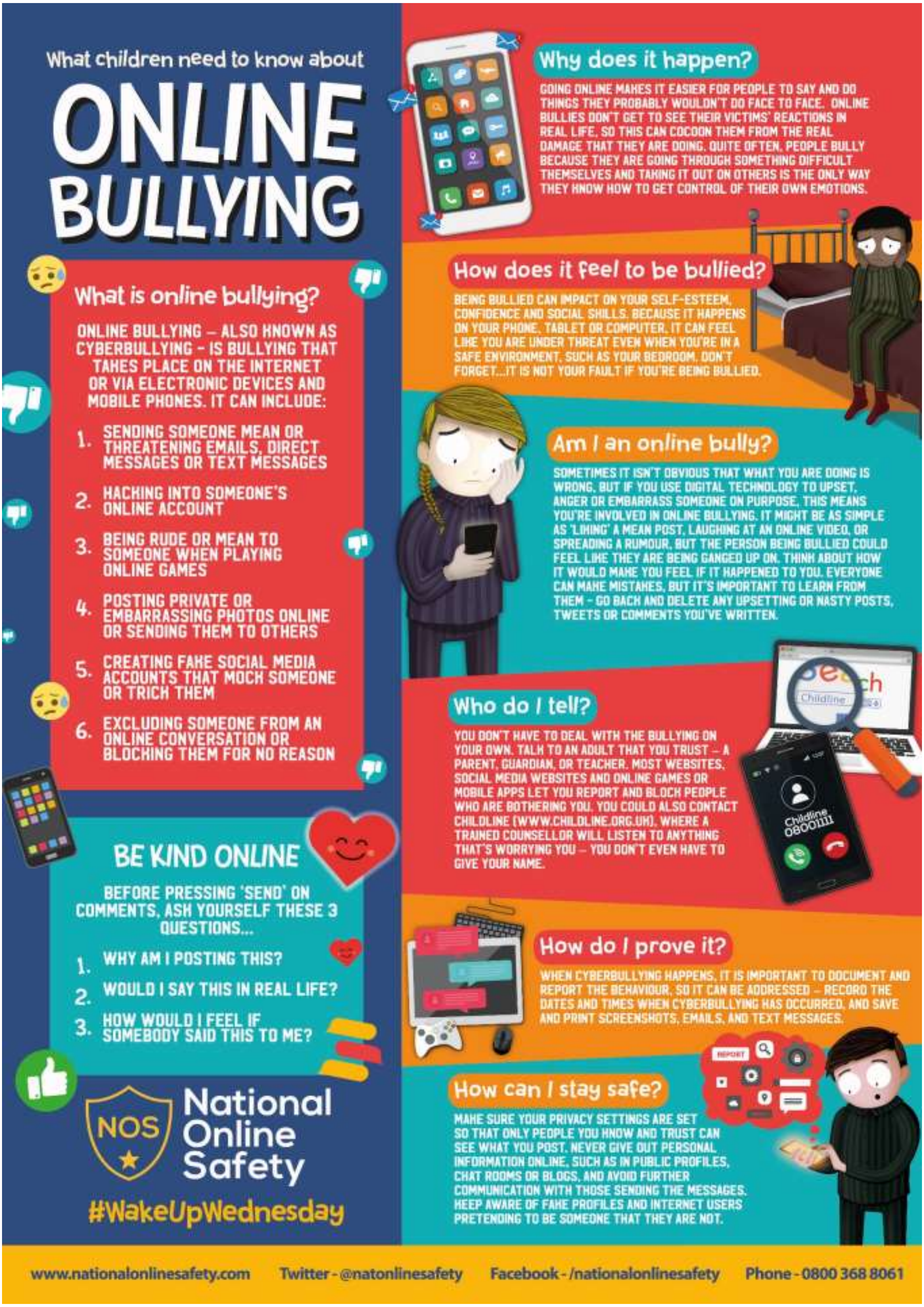
Monitoring and reviewing

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (ie ISP, school network or managed service as appropriate).
- Internal monitoring data for network activity.
- Surveys/questionnaires of pupils, parents/carers and staff.

The policy will be reviewed by the governors annually, or more regularly, in the light of any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to online safety as advised by the online safety committee or others.

Appendix 1 – Online bullying



What children need to know about

ONLINE BULLYING

What is online bullying?

ONLINE BULLYING – ALSO KNOWN AS CYBERBULLYING - IS BULLYING THAT TAKES PLACE ON THE INTERNET OR VIA ELECTRONIC DEVICES AND MOBILE PHONES. IT CAN INCLUDE:

1. SENDING SOMEONE MEAN OR THREATENING EMAILS, DIRECT MESSAGES OR TEXT MESSAGES
2. HACKING INTO SOMEONE'S ONLINE ACCOUNT
3. BEING RUDE OR MEAN TO SOMEONE WHEN PLAYING ONLINE GAMES
4. POSTING PRIVATE OR EMBARRASSING PHOTOS ONLINE OR SENDING THEM TO OTHERS
5. CREATING FAKE SOCIAL MEDIA ACCOUNTS THAT MOCK SOMEONE OR TRICK THEM
6. EXCLUDING SOMEONE FROM AN ONLINE CONVERSATION OR BLOCKING THEM FOR NO REASON

BE KIND ONLINE

BEFORE PRESSING 'SEND' ON COMMENTS, ASK YOURSELF THESE 3 QUESTIONS...

1. WHY AM I POSTING THIS?
2. WOULD I SAY THIS IN REAL LIFE?
3. HOW WOULD I FEEL IF SOMEBODY SAID THIS TO ME?

Why does it happen?

GOING ONLINE MAKES IT EASIER FOR PEOPLE TO SAY AND DO THINGS THEY PROBABLY WOULDN'T DO FACE TO FACE. ONLINE BULLIES DON'T GET TO SEE THEIR VICTIMS' REACTIONS IN REAL LIFE, SO THIS CAN COCOON THEM FROM THE REAL DAMAGE THAT THEY ARE DOING. QUITE OFTEN, PEOPLE BULLY BECAUSE THEY ARE GOING THROUGH SOMETHING DIFFICULT THEMSELVES AND TAKING IT OUT ON OTHERS IS THE ONLY WAY THEY KNOW HOW TO GET CONTROL OF THEIR OWN EMOTIONS.

How does it feel to be bullied?

BEING BULLIED CAN IMPACT ON YOUR SELF-ESTEEM, CONFIDENCE AND SOCIAL SKILLS. BECAUSE IT HAPPENS ON YOUR PHONE, TABLET OR COMPUTER, IT CAN FEEL LIKE YOU ARE UNDER THREAT EVEN WHEN YOU'RE IN A SAFE ENVIRONMENT, SUCH AS YOUR BEDROOM. DON'T FORGET...IT IS NOT YOUR FAULT IF YOU'RE BEING BULLIED.

Am I an online bully?

SOMETIMES IT ISN'T OBVIOUS THAT WHAT YOU ARE DOING IS WRONG, BUT IF YOU USE DIGITAL TECHNOLOGY TO UPSET, ANGER OR EMBARRASS SOMEONE ON PURPOSE, THIS MEANS YOU'RE INVOLVED IN ONLINE BULLYING. IT MIGHT BE AS SIMPLE AS 'LIKING' A MEAN POST, LAUGHING AT AN ONLINE VIDEO, OR SPREADING A RUMOUR, BUT THE PERSON BEING BULLIED COULD FEEL LIKE THEY ARE BEING GANGED UP ON. THINK ABOUT HOW IT WOULD MAKE YOU FEEL IF IT HAPPENED TO YOU. EVERYONE CAN MAKE MISTAKES, BUT IT'S IMPORTANT TO LEARN FROM THEM - GO BACK AND DELETE ANY UPSETTING OR NASTY POSTS, TWEETS OR COMMENTS YOU'VE WRITTEN.

Who do I tell?

YOU DON'T HAVE TO DEAL WITH THE BULLYING ON YOUR OWN. TALK TO AN ADULT THAT YOU TRUST – A PARENT, GUARDIAN, OR TEACHER. MOST WEBSITES, SOCIAL MEDIA WEBSITES AND ONLINE GAMES OR MOBILE APPS LET YOU REPORT AND BLOCK PEOPLE WHO ARE BOTHERING YOU. YOU COULD ALSO CONTACT CHILDLINE (WWW.CHILDLINE.ORG.UK), WHERE A TRAINED COUNSELLOR WILL LISTEN TO ANYTHING THAT'S WORRYING YOU – YOU DON'T EVEN HAVE TO GIVE YOUR NAME.

How do I prove it?

WHEN CYBERBULLYING HAPPENS, IT IS IMPORTANT TO DOCUMENT AND REPORT THE BEHAVIOUR, SO IT CAN BE ADDRESSED – RECORD THE DATES AND TIMES WHEN CYBERBULLYING HAS OCCURRED, AND SAVE AND PRINT SCREENSHOTS, EMAILS, AND TEXT MESSAGES.

How can I stay safe?

MAKE SURE YOUR PRIVACY SETTINGS ARE SET SO THAT ONLY PEOPLE YOU KNOW AND TRUST CAN SEE WHAT YOU POST. NEVER GIVE OUT PERSONAL INFORMATION ONLINE, SUCH AS IN PUBLIC PROFILES, CHAT ROOMS OR BLOGS, AND AVOID FURTHER COMMUNICATION WITH THOSE SENDING THE MESSAGES. KEEP AWARE OF FAKE PROFILES AND INTERNET USERS PRETENDING TO BE SOMEONE THAT THEY ARE NOT.

NOS National Online Safety

#WakeUpWednesday

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /nationalonlinesafety Phone - 0800 368 8061

Appendix 2 - Acts of Parliament relevant to online safety in schools

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 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.)

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 (eg using someone else's password to access files).
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program (eg 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.

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 judgment. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film 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.

Counter-Terrorism and Security Act 2015 (section 26)

The prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 empowers courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Criminal Justice and Immigration Act 2008 (section 63)

It is an offence to possess an 'extreme pornographic image'. An extreme pornographic image is defined in section 63 of this Act. Penalties can be up to three years imprisonment.

Data Protection Act 1998 (GDPR from May 2018)

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

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to cyber-bullying/bullying:

Executive Principals have the power ‘to such an extent as is reasonable’ to regulate the conduct of pupils off-site.

School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) 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 can include racist, xenophobic and homophobic comments, messages etc.

Obscene Publications Act 1959 and 1964

Publishing an ‘obscene’ article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he 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.

This also includes incidents of racism, xenophobia and homophobia.

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.

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.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) 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.

However, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 permit a degree of monitoring and record keeping, (eg 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.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as 'sexting'). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Appendix 3 - Useful organisations/support services for reporting online safety issues

Grooming or other illegal behaviour

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to *Child Exploitation Online Protection Centre (CEOP)*. See www.ceop.gov.uk.

Criminal content online

If you stumble across criminal content online, you should report this to the *Internet Watch Foundation (IWF)* at www.iwf.org.uk/report. Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.

On-line content which incites hatred on the grounds of race, religion and sexual orientation should be reported to *True Vision*, which tackles all forms of hate crime, including those on the grounds of disability and transgender identity. True Vision, at www.report-it.org.uk, will give you information on content which incites hatred and how to report it.

Scams

If you have been 'scammed, ripped off or conned' you can report to *Action Fraud* on 0300 123 2040 or http://www.actionfraud.police.uk. This service is run by the National Fraud Authority, the UK's government agency that helps coordinate the fight against fraud.

Getting help/advice: for young people

- ChildLine: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.**Getting help/advice: for parents**
- If you want to make a complaint about an advert, television or radio programme, film, newspaper, magazine, video game or other type of content that you think is unsuitable for children to see or hear, you can report it through ParentPort at www.parentport.org.uk. Click on 'Make a Complaint' and ParentPort will take you straight to the right place to complain to.
- Family Lives: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk
- Kidscape: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 5pm, Mondays and Tuesdays on 0207 823 5430 www.kidscape.org.uk.
- Childnet International Is a non-profit organisation working to help make the internet a safe place for children. 'We strive to take a balanced approach, making sure that we promote the positive opportunities, as well as responding to the risks and equipping children and young people to deal with them'. Contact details are: www.childnet.com phone 020 7639 6967, email info@childnet.com.
- UK council for child internet safety (UKCCIS) has practical guides to help parents and others with internet safety www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.
- Thinkuknow has a section for parents which offers advice on protecting children from abuse online offered by the National Crime Agency's CEOP Command www.thinkuknow.co.uk/parents.

Getting help/advice: for teachers

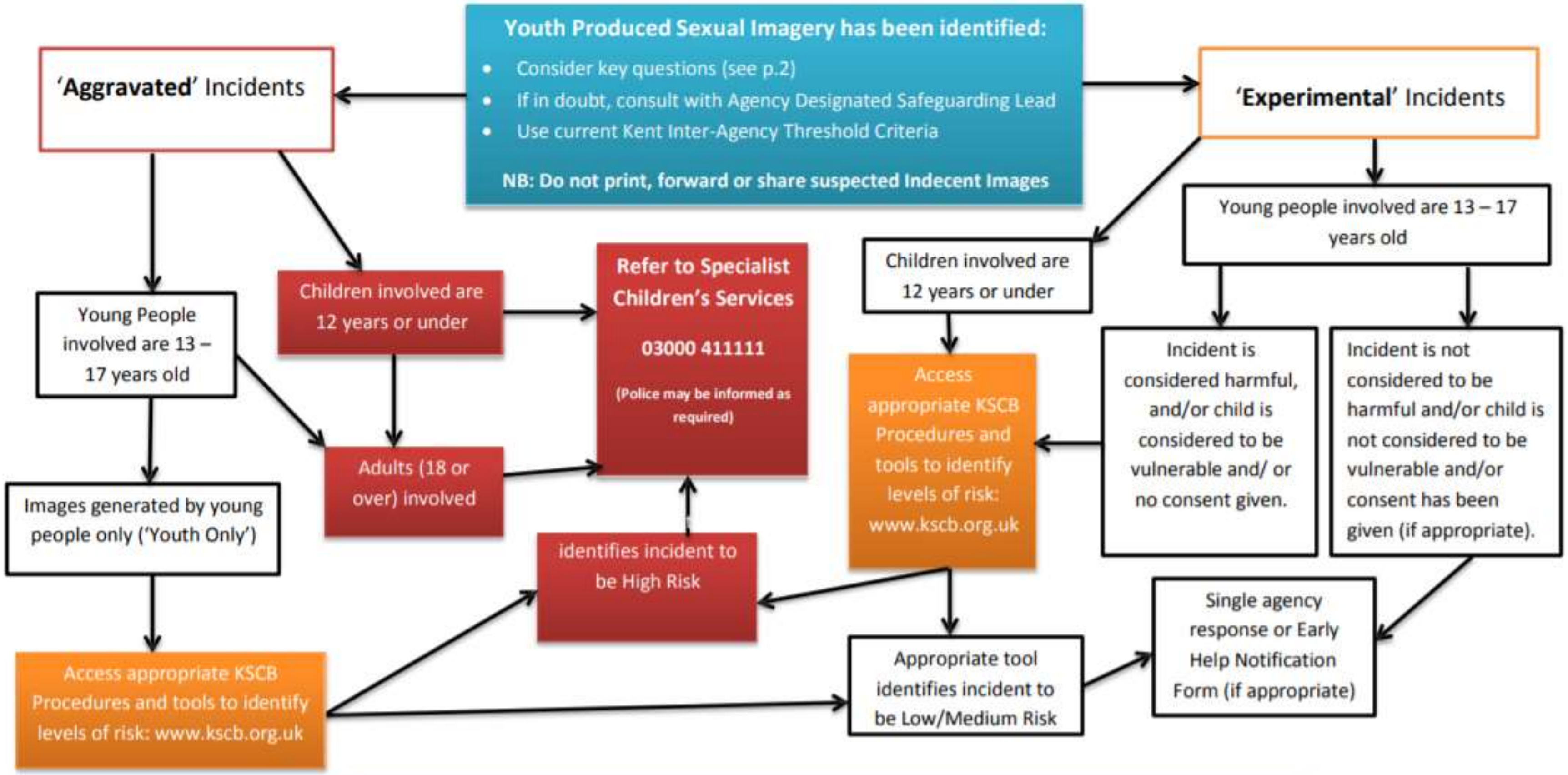
- DFE has a telephone helpline (0207 340 7264) and an email address (counter.extremism@education.gsi.gov.uk) to enable teachers to raise concerns or questions directly with them.

Getting help/advice: for professionals working with children

- Professionals online safety helpline: Helpline operated by the UK Safer Internet Centre offering professionals who work with children across the UK support, advice and mediation with on-line safety issues www.saferinternet.org.uk. The helpline can be contacted by email: helpline@saferinternet.org.uk or telephone on 0344 381 4772 (calls on this number are charged at local call rate)

Appendix 4 – Responding to youth produced sexual imagery

Responding to Youth Produced Sexual Imagery



Youth Produced Sexual Imagery has been identified:

- Consider key questions (see p.2)
- If in doubt, consult with Agency Designated Safeguarding Lead
- Use current Kent Inter-Agency Threshold Criteria

NB: Do not print, forward or share suspected Indecent Images

'**Aggravated**' Incidents

Young People involved are 13 – 17 years old

Images generated by young people only ('Youth Only')

Access appropriate KSCB Procedures and tools to identify levels of risk: www.kscb.org.uk

Children involved are 12 years or under

Adults (18 or over) involved

Refer to Specialist Children's Services

03000 411111

(Police may be informed as required)

identifies incident to be High Risk

'**Experimental**' Incidents

Children involved are 12 years or under

Access appropriate KSCB Procedures and tools to identify levels of risk: www.kscb.org.uk

Young people involved are 13 – 17 years old

Incident is considered harmful, and/or child is considered to be vulnerable and/ or no consent given.

Incident is not considered to be harmful and/or child is not considered to be vulnerable and/or consent has been given (if appropriate).

Appropriate tool identifies incident to be Low/Medium Risk

Single agency response or Early Help Notification Form (if appropriate)

Appropriate guidance and risk assessment tools may include:

- "Sexting in schools: youth produced sexual imagery and how to handle it": www.e-safety.org.uk
- KSCB Child Sexual Exploitation Toolkit
- KSCB 2.2.2 Children Who Exhibit Harmful Behaviour Including Sexual Harm (assessing and providing interventions)*
- KSCB 2.2.7 Working with Sexually Active Young People*
- KSCB 2.2.10 Online Safety, Child Abuse and Technology*
- Brook Traffic Lights tool https://www.brook.org.uk/our-work/category/sexual-behaviours-traffic-light-tool
- Kent Inter-Agency Threshold Criteria http://www.kscb.org.uk/guidance/kent-threshold-criteria

***All procedures are available at http://www.proceduresonline.com/kentandmedway**

Kscb/2016/april/jcra/version5

KSCB