Sir Roger Manwood's School

Online Safety Policy and Guidance for Education Settings

Date of Approval: January 2017

Date of Next Review: January 2019

Contents

1. Creating an Online Safety Ethos

1.1. Aims and policy scope

Sir Roger Manwood’s School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Sir Roger Manwood’s School believes that it has a duty to provide the school community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

The purpose of this online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Sir Roger Manwood’s School is a safe and secure environment.
- Safeguard and protect all members of Sir Roger Manwood’s School community online.
- Raise awareness of the potential risks as well as benefits of technology with members of Sir Roger Manwood’s School community.
- Enable staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures for members of the community to use when responding to online safety concerns.

This policy applies to all staff and other individuals who work for or provide services on behalf of the school (collectively referred to as ‘staff‘ in this policy) as well as children and parents/carers.

It applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) the Safeguarding and Child Protection Policy and the Acceptable Use Policy.

1.2. Writing and reviewing the online safety policy

Our online safety policy has been written by the school building on the Kent County Council (KCC) online safety policy template and government guidance.

The policy has been approved and agreed by the Senior Leadership Team and Governing Body and is available to stakeholders.

The Governor responsible for safeguarding (Ms Waite) takes lead responsibility for on-line safety.

Christine Buchanan is the appointed online safeguarding lead.

The school's online safety (e–Safety) Policy and its implementation will be reviewed biannually or sooner if required.

2. Online Communication and Safer Use of Technology

2.1. Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE). (NB this statement is specific to schools, however will an up-to-date website is viewed as good practice for early years settings)
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher/manager will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The school website will comply with the guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- The administrator account for the school website will be safeguarded with an appropriately strong password.

2.2. Publishing pupil images

- Images or videos that include pupils will be selected carefully and pupils' full names will not be used.
- Written permission from parents of carers will be obtained prior to publication of images or videos. This will be requested when pupils enter the school.

2.3. Managing email

- Pupils may only use school provided email accounts for educational purposes (remove for early years settings)
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.

- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- School email addresses and other official contact details will not be used for setting up personal social media accounts, unless this approved by SLT for official school purposes.

2.4. Official videoconferencing and webcam use for educational purposes (not currently in use)

- All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing involving pupils will be supervised by a member of staff.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.

- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference.

2.5. Appropriate and safe classroom use of the (Boarding) internet and any associated devices

- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with safety and security measures in place.
- Members of staff are expected to evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

2.6. Management of school learning platforms/portals/gateways

- Staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled unless it is required for operational purposes.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    a. The user will be asked to remove any material deemed to be inappropriate or offensive.
    b. The material will be removed by the site administrator if the user does not comply.
    c. Access to the LP for the user may be suspended.
    d. The user will need to discuss the issues with the appropriate member of staff before reinstatement.
    e. A pupil's parent/carer may be informed.

- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of Sir Roger Manwood's School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of Sir Roger Manwood's School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Sir Roger Manwood's School community.
- All members of Sir Roger Manwood's School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems
- Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of Sir Roger Manwood's School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2. Official use of social media

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes.
- Official use of social media sites as communication tools will be risk assessed and formally approved by a member of SLT or the IT Manager.

- Staff will use school provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.

3.3. Staff personal use of social media

- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current pupils, unless these pupils are family members, via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this should be discussed with Designated Safeguarding Lead and/or the Headteacher.
- All communication between staff and members of the school community on school business will take place via official approved channels.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher/manager.
- Any communication from pupils/parents received on personal social media accounts should be reported to the schools designated safeguarding lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional and the wider professional and legal framework.
- Members of staff will notify the DSL or Headteacher immediately if they consider that any content shared or posted via any information and communications

technology, including emails or social networking sites conflicts with their role in the school.

- Members of staff are encouraged not to identify themselves as employees of Sir Roger Manwood's School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.

3.4. Staff official use of social media

- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the head teacher/manager of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
- All staff will agree to follow the official Acceptable Use Policy.

3.5. Pupils use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites at school, will be dealt with in accordance with existing legal frameworks and school policies. Parents/carers may need to be involved.
- Depending on the issues arising, the School may also need to be involved in addressing on-line behaviours outside the school environment. These behaviours will also be dealt with in accordance with legal frameworks and existing school policies.

4. Use of Personal Devices and Mobile Phones

4.1. Rationale regarding personal devices and mobile phones

- Sir Roger Manwood's School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use Policy.

4.2. Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law, Acceptable Use and other school safeguarding policies.
- Electronic devices of all kinds that are brought on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.
- Members of staff will be issued with a work phone number and email address where contact with pupils or parents/carers is required.

4.3. Pupils use of personal devices and mobile phones

- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If a pupil needs to contact his/her parents/carers they will be allowed to use the school office phone under supervision of the main school office staff.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy. For continuous breaches of school policy, pupils will be directed to leave their phones at home or if deemed necessary to store them in the School Office during school hours.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer and content may be deleted or requested to be deleted, if appropriate.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then it may be necessary to hand the device over to the police for further investigation.

4.4. Staff use of personal devices and mobile phones

- Members of staff are normally not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. An exception to this is in the event of an emergency during a school visit when no suitable device is available.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law.
- Staff should not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school policy.

4.5. Visitors use of personal devices and mobile phones

- Parents/carers and visitors on the school site/accompanying trips/visits must use mobile phones and personal devices in accordance with the school Acceptable Use Policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- Sir Roger Manwood's School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- Methods to identify, assess and minimise online risks will be reviewed by the schools leadership team.

5.2. Internet use throughout the wider school community

- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- The school will expect any guest/visitor to who needs to access the school computer system or internet site to follow the Acceptable Use Policy.

5.3. Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All users will read and agree to follow the Acceptable Use Policy before using any school resources.
- When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1. Engagement and education of children and young people

- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Acceptable Use expectations and Posters will be posted in rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the schools internal online safety (e-Safety) education approaches.

6.2. Engagement and education of children and young people considered to be vulnerable

- Sir Roger Manwood's School is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate e.g. SENCO.

6.3. Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.

6.4. Engagement and education of parents and carers

- Sir Roger Manwood's School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- A partnership approach to online safety at home and at school with parents will be encouraged. Parents will be requested to read online safety information as part of the Home School Agreement and will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

7. Managing Information Systems

7.1. Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

7.2. Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- From year 7, all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- We require staff to change their passwords every 3 months.

7.3. Filtering and Monitoring

- The governors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- All users will be informed that use of school systems will be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our pupils.
- The school uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school will work with KCC and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead/IT Manager and will be addressed as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

7.4. Management of applications (apps) used to record children's progress

The school does not currently use apps to record progress but if they do the following guidance will be implemented.

- The Headteacher/manager is ultimately responsible for the security of any data or images held of children.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.

8. Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded and dealt with as appropriate.

- Any complaint about staff misuse will be referred to the DSL and head teacher and approached in-line with KCC guidelines.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Kent.
- Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

9. Procedures for Responding to Specific Online Incidents or Concerns

This guidance applies to all agencies working with children and young people and includes (but is not limited to) schools, early years settings, youth hubs, libraries, early help and preventative services.

9.1. Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

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.

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).

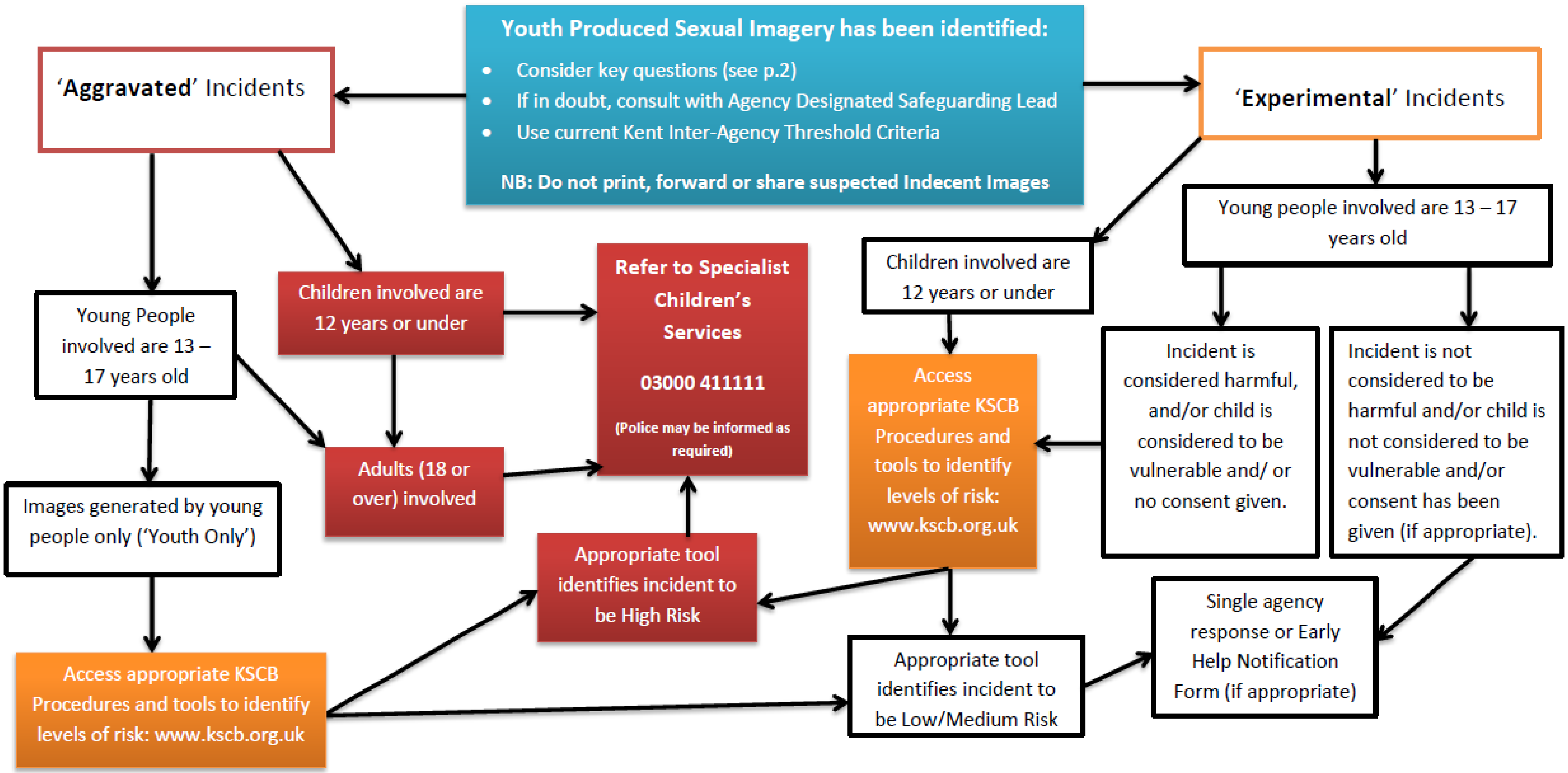
Professionals should be aware the prosecution or criminalisation of children for taking indecent images of themselves and sharing them should be avoided where possible. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children and young people especially 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.

If the school is made aware of incident involving creating youth produced sexual imagery the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the designated safeguarding lead.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.

- Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- Where deemed necessary, the school will inform parents/carers about the incident and how it is being managed.
- The school will not view an image suspected of being youth produced sexual imagery unless there is a clear need or reason to do so.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- If an indecent image has been taken or shared on the school network or devices then the school will take action to block access to all users and isolate the image.
- The school will ensure that members of the community are aware of sources of support regarding youth produced sexual imagery.
- The school will follow the guidance in the KSCB flow chart: Responding to Youth Produced Sexual Imagery and the UKCCIS Sexting in schools and colleges: Responding to incidents and safeguarding young people. This can be found by following this link: www.kcsb.org.uk/__data/assets/pdf_file/0006/60909/Sexting-KCSB-version-5-final.pdf.

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

Children involved are 12 years or under

Adults (18 or over) involved

Images generated by young people only (‘Youth Only’)

Refer to Specialist Children’s Services

03000 411111

(Police may be informed as required)

Appropriate tool identifies incident to be High Risk

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

‘**Experimental**’ Incidents

Young people involved are 13 – 17 years old

Children involved are 12 years or under

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).

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

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

9.2. Key questions – Responding to Youth Produced Sexual Imagery

Key questions to answer should include:	
What is already known about the child(ren) or young people involved?	• Age of child(ren) or young people • Previous/current agency involvement • Vulnerability e.g. special educational needs, child in care etc.? • Immediate risk of harm • Multiple incidents
How has the imagery been shared?	• Public or private • Apps/services involved
What do we know about the intent or motivation behind creating or sharing the imagery?	• Adult involvement • Coercion or blackmail • Ability to "consent" • Image is extreme or violent
What is the impact on the child(ren) or young people involved?	• Emotional impact • Criminal consequences • Potential long term impact

9.3. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- Sir Roger Manwood's School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.
    - Immediately inform Kent police via 101 (using 999 if a child is at immediate risk)
    - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care (if needed/appropriate).

    - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

9.4. Responding to concerns regarding Indecent Images of Children (IIOC)

- The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the local authority safeguarding team.
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.

  - Inform the police via 101 (999 if there is an immediate risk of harm) and children’s social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority safeguarding team and other relevant organisations in accordance with the schools managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

9.5. Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.

9.6. Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of Sir Roger Manwood’s School community will not be tolerated.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
  - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
  - Parent/carers of pupils involved in online bullying are likely to be informed.

  - The Police may be contacted.

9.7. Responding to concerns regarding online hate

- Online hate at Sir Roger Manwood’s School will not be tolerated and all members of the community will be advised to report any incidences.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Kent Police.

Appendix B

Online Safety (e-Safety) Contacts and References

Kent Support and Guidance

Kent County Councils Education Safeguards Team:
www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

Kent Online Safety Support for Education Settings

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
- esafetyofficer@kent.gov.uk Tel: 03000 415797

Kent Police:
www.kent.police.uk or www.kent.police.uk/internetsafety
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kent e–Safety Blog: www.kentesafety.wordpress.com

EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/