E-SAFETY POLICY INCL. YOUTH PRODUCED SEXUAL IMAGERY (YPSI) & SEXTING

Policy area

Safeguarding

Statutory regulation

Keeping Children Safe In Education, Sept 2025
Meeting Digital & Technology Standards in Schools & Colleges – DfE March 2023
UK Council for Internet Safety, UKCIS, Dec 2020

SLT Lead

Assistant Headteacher, Personalised Learning [SENCo] (Daniel Love)

Last Updated

July 2025

Last Approved

Approved by Council October 2025

Next review

September 2026

THE KING ALFRED SCHOOL
E-SAFETY POLICY INCL. YOUTH PRODUCED SEXUAL IMAGERY (YPSI)
& SEXTING

INTRODUCTION

King Alfred School (KAS) adopts a whole school approach to online safety and makes sure it is reflected in all policies, curriculum, teacher training, the role of DSL and parental engagement. The use of technology has become a significant component of many safeguarding issues, and it is essential that children are safeguarded from potentially harmful and inappropriate online material.

KAS works to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

KAS constantly reviews its online safety policies and information to reflect and keep up with developments in new technologies which are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music/video/image downloads;
- Gaming sites;
- Text messaging and picture messaging, including group chats ;
- Video calls;
- Podcasting;
- Online communities via interest groups, including but not limited to video games on consoles and PC/Mac, as well as associated services such as Discord and Twitch ;
- Mobile internet devices such as smart phones and tablets.
- Artificial Intelligence powered services, for example ChatGPT
- Video sharing services, for example YouTube

This policy, supported by the Acceptable IT Use policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Acceptable IT Use Policy;
- Anti-Bullying Policy;
- Behaviour Policy;
- Child on Child Abuse Policy;
- Complaints Procedure;
- Data Protection Policy;
- EYFS Policy;
- Health and Safety Policy;
- PSHE Policy;
- Safeguarding and Child Protection Policy;

- Staff Code of Conduct.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At KAS, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

SCOPE OF THIS POLICY

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, Council, and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable IT Use Policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

ROLES AND RESPONSIBILITIES

Council

Council, as the governing body of the school, is responsible for the approval of this policy and for reviewing its effectiveness. Council reviews this policy on a three year basis.

Head and the Senior Leadership Team

The Head is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Head has delegated day-to-day responsibility to the Assistant Headteacher, Personalised Learning [SENCo]. In particular, the role of the Head and the Senior Leadership team is to ensure that:

- the DSL is trained in Level 3 Safeguarding and e-safety, and
- staff, in particular the Assistant Headteacher, Personalised Learning [SENCo] are adequately trained about e-safety; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

Assistant Headteacher, Personalised Learning [SENCo]

The School's Assistant Headteacher, Personalised Learning [SENCo] is responsible to the Head for the day to day issues relating to e-safety. The Assistant Headteacher, Personalised Learning [SENCo] has responsibility for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, NCA, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board (Barnet MASH).

IT staff

The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and in part for training the school's teaching and administrative staff in the use of IT.

Teaching and support staff

All staff are required to confirm the Acceptable IT Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis. Staff must report issues of concern to the relevant Head of Year and the Assistant Headteacher, Personalised Learning [SENCo] and/or DSL.

Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable IT Use Policy, and for letting staff know if they see IT systems being misused.

Parents and carers

KAS believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

FILTERING & MONITORING

The school does all that it reasonably can to limit children's exposure to risks by having a robust monitoring and filtering system in place on all school devices and wi-fi. This system conforms to or exceeds all aspects of the governments **Filtering and Monitoring Standards for Schools and Colleges**. The use of the internet is monitored via an external Forensic E-Safety organisation in addition to on-site filtering and threat protection technologies. Inappropriate usage will be flagged immediately by the Forensic Monitoring Solution and reported directly in the first instance to the DSL and Assistant Headteacher Personalised Learning [SENCo] and ICT Department, or other members of staff as appropriate to the level of concern. The school is aware that risks and harms related to technology evolve rapidly and carries out an annual review of online safety which is supported by an annual risk assessment that considers and reflects on the risks the children face. In turn, these are supported by continual improvements to the school's hardware and software infrastructure in response to emerging concerns and pedagogical/technological developments.

Commented [TP1]: new piece

EDUCATION AND TRAINING

Staff: awareness and training

New staff receive information on the school's E-Safety and Acceptable IT Use policies as part of their induction together with information about their own personal IT use (Sexting & Social Media Risks for Staff) and further e-safety information in the Staff Code of Conduct.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time where appropriate and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable IT Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines and to explain that each school device has forensic monitoring.

Teaching staff are expected to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible via My Concern (safeguarding reporting) if any incident relating to e-safety occurs and be provided directly to appropriate staff including the DSL, relevant Head of Year and Assistant Headteacher, Personalised Learning [SENCo].

Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in callovers, as well as informally when opportunities arise.

At a minimum, the E-Safety Curriculum covers:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Commented [TP2]: new comment

At age-appropriate levels, and usually via PSHE, pupils are taught about their e-safety responsibilities and to look after their own online safety. Pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to their Form Tutor, Head of Year, the Designated Safeguarding Lead (DSL), and any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities. They are also taught about what constitutes illegal sexting and the subsequent consequences of such actions.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy and Child on Child Abuse Policy which describe the preventative measures and the procedures that will be followed when the school discovers cases of bullying or child on child abuse). Pupils should approach their Form Tutor, Head of Year, or Assistant Headteacher, Personalised Learning [SENCo] as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

The school is trialling the use of AI in different areas of the curriculum to educate students regarding the safe, ethical and responsible use of AI technology. This developing curriculum aspect is aligned with the government issued guidance: 1. 2.

Commented [TP3]: new comments

Online learning: If children are being asked to learn online at home, for example because of Covid 19, the school follows advice from the DfE on safeguarding and remote education and this can be found in the Acceptable Use of IT policy.

Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The DfE has produced a document on Harmful online challenges and online hoaxes - GOV.UK (www.gov.uk) which shares information for parents and carers and signposts where to get support. In addition the school stays in regular contact with parents to reinforce the importance of children's online safety, and runs regular parent forums to explain and update them on the latest online issues. It is important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school (if anyone) their child is going to be interacting with online.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges discussion evenings for parents where either staff or an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity. The DSL and other members of staff with specialist knowledge (e.g. Digital Literacy Co-Ordinator) sends out bulletins outlining the latest worrying Apps, Games, Trends/Challenges and Websites/Services.

POLICY STATEMENTS

Use of school and personal devices

Staff
We believe our staff should be completely attentive during their hours of work to ensure all children, including the EYFS, receive good quality care and education.

Therefore:

- Handheld devices/Personal mobile phones must not be used when working with children.
- Handheld devices/Personal mobiles must be kept on silent during working hours and be kept out of sight when working with children.
- Handheld devices/Personal mobiles may only be used on a designated break and, in the EYFS setting, only in a child free area (e.g. the staff rooms)
- Where possible, a designated school mobile only should be used on all school outings. However, in the event that this is not available staff may use personal mobiles on outings for emergency use only.
- Personal mobiles must never be used to take photographs of any of the children.

The Head, the Head of Lower School and the EYFS Coordinator reserve the right to check the image contents of a member of staff's mobile phone should there be any cause for concern over its appropriate use.

Should inappropriate material be found then our Local Authority Designated Officer (LADO) will be contacted immediately.

We will follow the Staff Code of Conduct and the LADO's guidance as to the appropriate measures to be taken.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents/carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system. See the Staff Code of Conduct for more information.

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Pupils

If pupils bring in mobile devices/smart phones (e.g. for use during the journey to and from school), they remain the responsibility of the child in case of loss or damage. Depending on their age, pupils are asked to submit their phones at the beginning of the school day for return later in the day.

School mobile technologies available for pupil use including laptops, tablets, cameras, etc. are stored in relevant, secure locations. Subject departments and relevant staff are responsible for devices allocated to their particular area of the school.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the relevant Head of Year to agree how the school can appropriately support such use. The Head of Year will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

The school also recognises that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. In these circumstances the procedures from the schools Child on Child Abuse incl. Sexual Violence and Sexual Harassment Policy will be followed.

Use of internet and email

Staff

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure using current up to date technologies such as Forensic Monitoring, Encryption, Filtering and password policies. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the DSL, Assistant Headteacher, Personalised Learning [SENCo] or Director of IT the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Assistant Headteacher, Personalised Learning [SENCo] or Director of IT.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring King Alfred School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent/carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils from Year 3 onwards are issued with their own personal school email addresses for use on our network and via cloud services. In addition, in Years 2 to 5, children are assigned a 1:1 ipad with access to the internet. All internet access on these devices is registered against the student's name on a database, ensuring accountability and protection. Access from Year 6 and on school computers is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all communication related to school work. Pupils should be aware that email communications through the school network and school email addresses are monitored. Students in Years 3-6 can only send and receive emails from people with our school accounts ending with '@kingalfred.org.uk'.

Commented [TP4]: procedural updates added

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work purposes, pupils should contact the ICT Service Desk for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to their Form Tutor, Head of Year, or Assistant Headteacher, Personalised Learning [SENCo].

The school expects pupils to think carefully before they post any information online or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others. Pupils understand that the creation of content for the purpose of sharing on social media on the school grounds is expressly forbidden, and that the unauthorised sharing of images/videos of underage children may be putting them at risk of legal action from third parties outside of the school's control.

Pupils must report any accidental access to materials of a violent or sexual nature directly to their Form Tutor, Head of Year, or Assistant Headteacher, Personalised Learning [SENCo], or any other member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its WIFI network is monitored.

Data storage and processing

The school takes its compliance with GDPR seriously. Please refer to the Data Protection Policy and the Acceptable IT Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to the school's central server or their own Microsoft 365 Cloud Environment. In the Lower School, staff and children are expected to use their Google Workspace for the same purposes.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Assistant Headteacher, Personalised Learning [SENCo].

Password security

Pupils from Year 3 to Year 5 have generic passwords that they use to log on to the desktop computers in school. They do not use passwords to logon to the internet when using their 1:1 ipads in class, instead these devices have their ID numbers associated with individual students. Students from Year 2 to Year 6 use their passwords to access their cloud services. Staff and pupils from Year 6 and above have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

Commented [TP5]: new

All pupils and members of staff should:

- use a strong password;
- not write passwords down; and

- not share passwords with other pupils or staff.

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy and the Acceptable IT Use Policy / EYFS Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Misuse

KAS will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or Barnet MASH. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the NCA or CEOP. If relevant, include the school's guidance on particular activities that would be illegal or classed as inappropriate and therefore restricted.

Incidents of misuse or suspected misuse, including Cybercrime (which is a criminal activity) will be dealt with by staff in accordance with the school's policies and procedures.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy and Peer on Peer Abuse Policy.

COMPLAINTS

As with all issues of safety at KAS, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Head in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate. Please see the Complaints Procedure for further information.

YOUTH PRODUCED SEXUAL IMAGERY (YPSI)
& SEXTING IN SCHOOLS

Definition of 'Sharing nudes and semi-nudes'

This advice uses the term 'sharing nudes and semi-nudes' to mean the sending or posting of nude or semi-nude images, videos or live streams by young people under the age of 18 online. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline.

The term 'nudes' is used as it is most commonly recognised by young people and more appropriately covers all types of image sharing incidents. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated. Such images may be created and shared consensually by young people who are in relationships, as well as between those who are not in a relationship. It is also possible for a young person in a consensual relationship to be coerced into sharing an image with their partner. Incidents may also occur where:

- children and young people find nudes and semi-nudes online and share them claiming to be from a peer.
- children and young people digitally manipulate an image of a young person into an existing nude online.
- images created or shared are used to abuse peers e.g. by selling images online or obtaining images to share more widely without consent to publicly shame.

Alternative definitions

Many professionals may refer to 'nudes and semi-nudes' as:

- youth produced sexual imagery or 'youth involved' sexual imagery (YPSI).
- indecent imagery. This is the legal term used to define nude or semi-nude images and videos of children and young people under the age of 18 (IIOC).
- 'sexting'. Many adults may use this term, however some young people interpret sexting as 'writing and sharing explicit messages with people they know' rather than sharing images.
- image-based sexual abuse. This term may be used when referring to the non-consensual sharing of nudes and semi-nudes.
- Terms such as 'revenge porn' and 'upskirting' are also used to refer to specific incidents of nudes and semi-nudes being shared. However, these terms are more often used in the context of adult-to-adult non-consensual image sharing offences outlined in s.33-35 of the Criminal Justice and Courts Act 2015, Voyeurism (Offences) Act 2019 and s.67A of the Sexual Offences Act 2003.

Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents involving children and young people complex. There are also a range of risks which need careful management from those working in education settings.

Incidents covered by the UKCCIS guidance:

- Person under 18 creates a sexual image of themselves and shares it with another person under 18.
- A person under 18s shares an image of another under 18 with another person under 18 or an adult.
- A person under 18 is in possession of sexual imagery created by another person under 18.

Incidents not covered by the UKCCIS guidance:

- Under 18s sharing adult pornography.
- Under 18s sharing sexual texts without sexual imagery.
- Adults sharing sexual imagery of under 18s (this is child sexual abuse and must always be reported to the police).

Response to incidents of youth produced sexual imagery (YPSI)

The response should be guided by the principle of proportionality - "The primary concern at all times should be the welfare and protection of the young people involved" *(Sharing Nudes & Semi Nudes: Advice for Schools Dec 2020)*.

It is important to place a child's sexual behaviour with the context of their age and development.

The Law

Making, possessing, and distributing any imagery of someone under 18 which is indecent is illegal. This includes images of yourself if you are under 18.

Indecent is not defined in law, but images are likely to considered indecent if they depict:

- A naked young person
- A topless girl
- An image which displays genitals, and
- Sex acts including masturbation
- Indecent images may also include overtly sexual images of young people in their underwear

These laws weren't created to criminalise young people but to protect them.

Although sharing sexual images of themselves is illegal and risky, it is often the result of curiosity and exploration. Young people need education, support, and safeguarding, not criminalisation.

The National Police Chiefs' Council (NPCC) is clear that "youth-produced sexual imagery should be primarily seen as a safeguarding issue".

Schools may respond to incidents without involving the police (However, in some circumstances the police must always be involved).

Crime Recording

When police are notified about youth-produced sexual imagery, they must record this as a crime. The incident is listed as a crime, and the young person is the suspect. This is, however, not the same as a criminal record.

Every crime report to the police must have an outcome code. The NPCC, Home Office and the DBS have agreed a new outcome code for youth-produced sexual imagery.

Outcome 21: this outcome code allows the police discretion not to take further action if it is not in the public interest, even though there is enough evidence to prosecute. Using this outcome code is likely to mean the offence would not appear on a future Enhanced DBS check, although not impossible, as that disclosure is a risk based decision. Schools can be assured that the police have the discretion they need not to adversely impact young people in the future.

If a crime has been committed then these become either:

- **Section 1 Offence:** Taking, Making & Possessing with intent, distribution and sharing of an image.
- **Section 160 Offence:** Possession of an image, kept on digital chats or camera roll.

Handling Incidents:

- Refer to DSL/Head
- Assess the Risks
- HoYs/DSL meet with the young people involved
- Do not view the image unless it is unavoidable
- Discuss with parents, unless there is an issue where that's not possible
- Any concern the young person is at risk of harm, contact social care or the police
- Support the young people involved
- Staff can seize any probhibited item found as a result of a search. They can also seize any item they consider harmful or detrimental to the school.

Schools can review phones and delete data **UNLESS REFERRING TO THE POLICE.**

Always refer to the police or social care if incident involves:

- An adult
- Aggravating factors i.e. Coercion, blackmail, grooming, adults, bait sites, exploitation, extensive sharing, inappropriate sharing, malicious intent, persistent behaviour, profit motive (age is not an aggravating factor),
- Concerns about capacity, consent
- Images show atypical sexual behaviour for the child's developmental age
- Violent acts are depicted
- Image shows sex acts and includes a child under 13
- A young person at risk of harm as a result of the disclosure (for example self- harm or suicide)

Once the DSL/Head has enough information, the decision should be made as to whether to deal with the matter in school, refer it to the police or to social care. All information and decision making should be recorded in line with school policy on My Concern. If the incident has been dealt with in school, a further review should be held to assess risks.

Assessing Risks once the images have been shared:

- Has it been shared with the knowledge of the young person?
- Are adults involved in the sharing?
- Was there pressure to make the image?
- What is the impact to those involved?
- Does the child or children have additional vulnerabilities?
- Has the child taken part in producing sexual imagery before?

Viewing images:

- Avoid viewing youth-produced sexual imagery. Instead, respond to what you have been told the image contains.
- If it is necessary to view, discuss with the Head first.
- Never copy, print or share the image (it's illegal)
- View with another member of staff present
- Record the fact that the images were viewed along with reasons and who was present. Sign and date.

Deleting images (from devices and social media)

If the school has decided that involving other agencies is not necessary, consideration should be given to deleting the images. It is recommended that pupils are asked to delete the images themselves to confirm they have done so. This should be recorded, signed and dated. Any refusal to delete the images should be treated seriously, reminding the pupil that possession is unlawful.

Summary:

- Not "sexting" but "youth produced sexual imagery".
- Although illegal, police involvement is not always necessary.
- Images can be deleted and incident managed in school.
- Risk-based approach.
- The safeguarding policy reflects this guidance and relevant safeguarding and pastoral staff are aware of it.