King's College
The British School of Madrid
Soto de Viñuelas

School Online Safety Policy (E-Safety)

Contents

King's College
The British School of Madrid
Soto de Viñuelas

5. Data Security

5.1 Management Information System access

5.2 Data transfer

5.3 Asset Disposal

6. Equipment and Digital Content

6.1 Personal mobile phones and devices

6.2 Digital images and video

Appendices:

A1: Pupils Appropriate Use of Technology Policy

A2: Website and Social Media Guidelines

A3: Digital Citizenship

A4: King's Group Mobile Phone Policy 2018

A5: King's Group Sexting Youth Produced Sexual Imagery Policy 2018

King's College
The British School of Madrid
Soto de Viñuelas

1. Introduction and Overview

1.1 Rationale and Scope

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community
- at King's College schools with respect to the use of IT-based technologies.
- Safeguard and protect children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of King's College schools (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of King's College schools IT systems, both in and out of the school.

1.2 Roles and responsibilities

Role	Key Responsibilities
Headteacher **Head of Secondary School** **Head of Primary School**	• Must be adequately trained in offline and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. Securly • To be responsible for ensuring that all staff receive suitable training • To carry out their safeguarding and online safety roles • To embed online safety in the curriculum • To be aware of procedures to be followed in the event of a serious online safety incident

King's College *The British School of Madrid* Soto de Viñuelas	• Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Digital Learning Coordinator or Director of Digital Learning • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. Network Manager or Director of Digital Learning • To ensure Senior Leadership Team are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school websites includes relevant information

Role	**Key Responsibilities**
Designated Safeguarding Lead (This may be the same person)	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community and ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident. e.g. MyConcern • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and is aware of the potential for serious child protection concerns.

King's College
The British School of Madrid
Soto de Viñuelas

Governors / Safeguarding & E-Safety Governor	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor who is also the Safeguarding link Governor will include: regular review with the Director of Digital Learning

Role	Key Responsibilities
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
Director of Digital Learning	• To report online safety related issues that come to their attention, to the schools DSL or SLT • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
Network Manager/ technician	• To report online safety related issues that come to their attention, to the schools DSL or SLT • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Head of Primary or Head of Secondary as appropriate

Commented [1]: Might need amending as Tom is leaving.

King's College *The British School of Madrid* Soto de Viñuelas	• To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Data Managers	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • To ensure that the school follows the current GDPR law with school data.

Role	Key Responsibilities
Teachers	• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the DSL/Head of Primary or Head of Secondary school • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology Exit strategy: At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to login and allow a factory reset.

Commented [2]: Is this part of the induction program for new staff?

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use of Technology Policy and the Website and Social Media Guidelines • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and 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 • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use of Technology Policy and Website and Social Media Guidelines Agreement with their child/ren • To consult with the school if they have any concerns about their children's use of technology • To support the school in promoting online safety with their child.
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

1.3 How the policy is communicated to staff / pupils / community

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

1.4 Handling Complaints

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Digital Learning Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported using the school's rewards and sanctions system.
- Any concern about staff misuse is always referred directly to the Headteacher, Head of Primary or Head of Secondary, unless the concern is about the Headteacher, Head of Primary or Head of Secondary in which case the complaint is referred to the Safeguarding & E-Safety Governor or Headteacher respectively.

Handling a sexting / nude selfie incident:

Please refer to the King's group Youth Produced Sexual Imagery Policy

1.5 Reviewing and Monitoring Online Safety

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

2.1 Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing or PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience; plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);

- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Commented [3]: Does this refer to the use of devices as well? Some pupils bring in their own device for certain subjects.

2.2 Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement, Erasmus and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

2.3 Parent awareness and training

This school:

- runs workshops on online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities.

4. Managing IT and Communication System

4.1 Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity;
- uses the Fortiguard filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- uses SOPHOS as a global antivirus solution for all King's Group schools for Windows computers.
- uses user-level filtering where relevant;
- secondary Pupils have a second layer of filtering via Securly when using Chromebooks. Securly monitors and notify the school of internet misuse. Parents can access to their child's/children's navigation history and manage the filtering settings they the Chromebook is used at home.
- ensures network health through use of anti-virus software;
- Uses secure file/email to send 'protect-level' (sensitive personal) data over the Internet.
- Uses Google as their teacher and pupil provider. Pupils can only send and receives emails from other pupils and teachers. The school can allow third party users to contact our pupils when it is necessary for educational purposes, e.g. Examination Boards, Inspection Boards, etc.
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;

4.2 Network management (user access, backup)

This school

- Uses individual, audited logins for all users;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations /viewing users/setting-up applications and Internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- Has daily backup of school data (admin and curriculum if need it);
- Uses secure, 'Cloud' storage for data backup that conforms to DfE guidance;

- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different/use the same username and password for access to our school's network;
- All pupils have their own unique username and password which gives them access to the Internet, unlimited storage in the Cloud, GSuite and other services.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer, laptop, chromebook, iPad or other device loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing King's College systems do so in accordance with any Corporate policies; e.g. King's College email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school approved systems;
- Does not allow any outside companies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote offsite backup of data;
- This school uses secure data transfer;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Commented [4]: Check up on this.

4.3 Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords twice a year.

4.4 E-mail

This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- We use anonymous group email addresses, for example soto.secondary@kings.education / alicante.y9a@kcpupils.org
- Will contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of technologies to help protect users and systems in the school, including desktop antivirus products, plus direct email filtering for viruses.

Pupils:

- We use an algorithm to create our pupils emails.
- Pupils can only be accessed by other pupils and teachers in the school. No external contact is allowed, only by necessary educational organisations like Examination boards, Inspection Bodies, etc.
- Pupils are taught about the online safety and 'netiquette' of using email both in school and at home.

Staff:

- Staff can only use King's Group email systems on the school system
- Staff will use King's Group email systems for professional purposes
- Access in school to external personal email accounts may be blocked
- Never use email to transfer staff or pupil personal data.

4.5 School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

4.6 Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

4.7 Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- For the use of any school approved social networking will adhere to school's communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;

- Personal opinions should not be attributed to the school and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our pupil Acceptable Use of Technology Agreement and the Website and Social Media Guidelines

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use of Technology Agreement and the Website and Social Media Guidelines as well as additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

4.8 CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety.
- The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security: Management Information System access and Data transfer

5.1 Management Information System access

At this school:

- Matthew Taylor is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record.

Commented [5]: Senior Information Risk Officer

5.2 Data Transfer

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.

5.3 Asset Disposal

- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

6. Equipment and Digital Content

6.1 Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff members, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Pupils are discouraged from bringing phones into school and if they are they must be off and out of site all day. Any phone that is seen will be immediately confiscated. Please see the Mobile Phone Policy for more information.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- All mobile devices will be placed in the locker should they be brought into school.
- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.

- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- Personal mobile devices will only be used during lessons with permission from the teacher as part of an approved and directed curriculum-based activity with consent from the Head of Primary or Head of Secondary School.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times from the Head of Primary or Secondary School or the Headteacher.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- Staff mobiles devices may be searched at any time as part of routine monitoring.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are prohibited from contacting their child via their mobile phone during the school day, but should contact the school office.

Commented [6]: Used by pupils in the library to listen to music.

Commented [7]: We may need to change the wording here.

Commented [8]: Parents sometimes contact older pupils through their mobile phone.

School Owned Mobile Devices

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the IT Technician.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the IT Technician.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.

- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide their own mobile number for confidentiality purposes and then report the incident to the Headteacher.
- If a member of staff breaches the school policy then disciplinary action may be taken.

6.2 Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Created and Reviewed by :	**Policy Category:**
Carlos Lázaro September 2018	
Approved by KGB: November 2018	**Next Review:** September 2019

King's College
The British School of Madrid
Soto de Viñuelas

Appendix A1:

Pupils Appropriate Use of Technology Policy

The purpose of this document is to inform parents, guardians and pupils of the rules governing the use of school and personal technology resources while on or near school property, in school vehicles and at school-sponsored activities, as well as the use of school technology resources via off-site remote access.

Introduction

King's College is pleased to offer pupils access to school computers, mobile devices, the Internet and an array of technology resources to promote educational excellence. Each pupil is responsible for her/his use of technology, whether personal or school-provided. While using school and personal technology resources on or near school property, in school vehicles and at school-sponsored activities, as well as using school technology resources via off-site remote access, each pupil must act in an appropriate manner consistent with school and legal guidelines. It is the joint responsibility of school personnel and the parent or guardian of each pupil to educate the pupil about his/her responsibilities and to establish expectations when using technology.

Using the Internet and Communications Systems

School technology resources are provided to pupils to conduct research, complete assignments, and communicate with others in furtherance of their education. **Access is a privilege, not a right;** as such, general rules of school behaviour apply. Access to these services is given to pupils who agree to act in a considerate and responsible manner. Just as pupils are responsible for good behaviour in a classroom or a school hallway, they must also be responsible when using school computer networks or personal technologies.

Pupils must comply with school standards and honour this agreement to be permitted the use of technology.

All digital storage on school servers and computers is school property, and as such, network administrators will review files and communications to maintain system integrity and ensure that pupils are using technology responsibly. Pupils should not expect that files stored on school servers or computers will be private.

The educational value of technology integration in curriculum is substantial. Access to the Internet enables students to use extensive online libraries and resources. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, profane, sexually oriented or potentially offensive to some people. While the intent is to make Internet access available to further educational goals and objectives, pupils may find ways to access these other materials as well. King's College does not condone or permit the use of this material and uses content filtering software to protect pupils to the extent possible. Parents and guardians must be aware that content filtering tools are not completely fail-safe and while at school, direct supervision by school personnel of each student using a computer is desired but not always possible. Pupils are expected to use technology resources in a manner consistent with the rules below and will be held responsible for their intentional misuse. King's College believes that the benefits of pupil access to the Internet in the form of information resources and opportunities for collaboration exceed disadvantages. Ultimately, parents and/or guardians are responsible for setting and conveying the standards that their children should follow when using technology. If a student accidentally accesses inappropriate material they should back out of that information at once and notify the supervising adult.

Proper and Acceptable Use of All Technology Resources

All school technology resources, including but not limited to school computers, Mobile Devices and the Internet, must be used in support of education and academic research and must be used in a manner consistent with the educational mission and objectives of King's College.

Activities that are permitted and encouraged include:

- school work;
- original creation and presentation of academic work;
- research on topics being studied in school;
- research for opportunities outside of school related to community service, employment or further education.

Activities that are not permitted when using school or personal technologies include but are not limited to:

- plagiarism or representing the work of others as one's own;
- using obscene language; harassing, insulting, ostracizing, or intimidating others;
- representing Copyright ©, Registered ®, and/or Trademark TM materials as one's own work;
- searching, viewing, communicating, publishing, downloading, storing, or retrieving materials that are not related to school work,
- damaging or modifying computers, tablets or networks;
- intentional or neglectful transmission of viruses or other destructive computer files; hacking into school or external computers or tablets
- intentionally bypassing school filters;
- use of USB, bootable CDs, or other devices to alter the function of a computer or a network;
- subscription to any online services or ordering of any goods or services;
- online sharing of any pupil's or staff member's name, home address, phone number or other personal information;
- non-educational uses such as games, role-playing multi-user environments, gambling, junk mail, chain mail, jokes or raffles;
- participating in online chat rooms, social networking sites or using instant messaging, unless specifically assigned by a teacher;
- use of school resources for commercial purposes, personal financial gain, or fraud;
- any activity that violates a school rule or a local, provincial or national law.
- recording of any kind of teachers and staff without previous consent.

Pupils are expected to report harassment, threats, hate-speech and inappropriate content to a teacher or administrator. If a pupil has any questions about whether a specific activity is permitted, he or she should ask a teacher or IT administrator.

Privacy and Security

Pupils must use school technologies responsibly and in a secure manner. They must not share their logins, passwords, or access with others. We use Securly to monitor 24/7 our pupils when using their Chromebooks. Parents have the ability to monitor and set filtering policies when Chromebooks are used at home.

Online Assessments

Pupils assessments may be conducted using technologies such as the Internet or audience response systems. Normally, pupils will use these technologies as a part of their instructional day. Privacy and security, as defined above, along with confidentiality of assessment responses, are expected.

Vandalism

Any intentional act by a pupil that damages school technology hardware, software, operating systems, or data will be considered vandalism and will be subject to school rules and disciplinary procedures. Any intentional act that requires a person's time to repair, replace, or perform corrective work on district technologies or data is also considered vandalism.

Consequences of Misuse

Misuse of personal or school technology resources while on or near school property, in school vehicles and at school-sponsored activities, as well as the use of school technology resources via off-site remote access may result in disciplinary action up to and including permanent exclusion. In addition, the pupil's use of school technologies may be suspended or restricted. A school may temporarily hold (pending parental or same-day pick up) personal technology resources that are used inappropriately. King's Group individual schools may choose to have additional rules and regulations pertaining to the use of personal, networked, and communications resources in their respective buildings. Furthermore, intentional unauthorized access and/or damage to networks, servers, user accounts, passwords, or other school resources may be punishable under local, provincial, or national law.

Reliability and Limitation of Liability

King's College makes no warranties of any kind, expressed or implied, for the technology resources it provides to pupils. King's College will not be responsible for any damages suffered by the pupil, including those arising from non-deliveries, misdeliveries or service interruptions to email, unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people. Use of any information obtained via the Internet or communications technologies is at the pupil's own risk. King's College specifically denies any responsibility for the accuracy or quality of information obtained through the Internet. The pupils and his/her parent/guardian will indemnify and hold King's College harmless from any losses sustained as the result of misuse of the school's technology resources by the pupil.

King's College
The British School of Madrid
Soto de Viñuelas

Appendix A2:

Website and Social Media Guidelines

Think before you act because your virtual actions are real and permanent.

- Be aware of what you post online. Website and social media venues are very public. What you contribute leaves a digital footprint for all to see. Do not post anything you wouldn't want friend, enemies, parents, teachers, future colleges, or employees to see. (THINK, Is it True, Helpful, Inspiring, Necessary, Kind?)
- Follow the school's code of conduct when writing online. It is acceptable to disagree with other's opinions; however, do it in a respectful way. Make sure that criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online.
- Be safe online. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birth dates, and pictures. Do not share your password with anyone besides your teachers and parents.
- Linking to other websites to support your thoughts and ideas is recommended. However, be sure to read and review the entire website prior linking to ensure that all information is appropriate for a school setting.
- Do your own work! Do not use other people's intellectual property without their permission. Be aware that it is a violation of copyright law to copy and paste others' thoughts. (Plagiarism) It is good practice to hyperlink to your sources.
- Be aware that pictures may also be protected under copyright laws. Verify that you have permission to use the image or that it is under Creative Commons attribution.
- How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity.
- Online work should be well written. Follow writing conventions including proper grammar, capitalisation, and punctuation. If you edit someone else's work, be sure it is in the spirit of improving and writing.
- If you come across inappropriate material that makes you feel uncomfortable or is not respectful, tell your teacher right away.
- Pupils are not allowed to change any Chrome settings without teacher permission. Only tool/apps setting changes are allowed.
- Pupils will have access to Youtube. They are expected to use it for school provided/related use only.
- Pupils are not allowed to mirror their computer screens to the school projectors without approval from the teacher.

King's College
The British School of Madrid
Soto de Viñuelas

Appendix A3:

Digital Citizenship

Appropriate Uses and Digital Citizenship

While working in a digital and collaborative environment, students should always conduct themselves as good digital citizens by adhering to the following:

1. Respect Yourself. I will show respect for myself through my actions. I will select online names that are appropriate. I will use caution with the information, images, and other media that I post online. I will carefully consider what personal information about my life, experiences, or relationships I post. I will not be obscene. I will act with integrity.

2. Protect Yourself. I will ensure that the information, images, and materials I post online will not put me at risk. I will not publish my personal details, contact details, or a schedule of my activities. I will report any attacks or inappropriate behavior directed at me while online. I will protect passwords, accounts, and resources.

3. Respect Others. I will show respect to others. I will not use electronic mediums to antagonize, bully, harass, or stalk people. I will show respect for other people in my choice of websites: I will not visit sites that are degrading to others, pornographic, racist, or inappropriate. I will not enter other people's private spaces or areas.

4. Protect Others. I will protect others by reporting abuse and not forwarding inappropriate materials or communications. I will avoid unacceptable materials and conversations.

5. Respect Intellectual property. I will request permission to use copyrighted or otherwise protected materials. I will suitably cite all use of websites, books, media, etc. I will acknowledge all primary sources. I will validate information. I will use and abide by the fair use rules.

6. Protect Intellectual Property. I will request to use the software and media others produce. I will purchase, license, and register all software or use available free and open source alternatives rather than pirating software. I will purchase my music and media and refrain from distributing these in a manner that violates their licenses.

Copyright and File Sharing

Students are required to follow all copyright laws around all media including text, images, programs, music, and video. Downloading, sharing, and posting online illegally obtained media is against the Acceptable Use of Technology Policy.

Monitoring Software

Teachers, management, and the technology department staff may use monitoring software that allows them to view the screens and activity on student Chromebooks.

Appendix A4:

Mobile Phone Policy

Mobile phones now include many additional functions such as an integrated camera, video recording capability, instant messaging, mobile office applications and mobile access to the internet. These allow immediate access to email, searching for information on the internet and other functions such as access to social networking sites e.g. Facebook, Twitter and blogging sites.

For many young people today the ownership of a mobile phone is considered a necessary and vital part of their social life. When used creatively and responsibly the smart phone has great potential to support a pupil's learning experiences.

In recent years schools have had incidents of poor conduct where mobile phone use has been a feature. This has been particularly difficult to address if it is an element in bullying. Bullying, intimidation and harassment are not new in society; however bullying using a mobile phone represents a new challenge for schools to manage.

Parents and pupils should be clear that misuse of mobile phones will not be tolerated. The following are examples of misuse but are not exclusive. 'Misuse' will be at the discretion of the Head:

- the deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience such as on Facebook or YouTube
- bullying by text, image and email messaging
- the use of a mobile phone for 'sexting' (the deliberate taking and sending of provocative images or text messages)
- pupils posting material on social network sites with no thought to the risks to their personal reputation and sometimes with the deliberate intention of causing harm to others
- making disrespectful comments, misrepresenting events or making defamatory remarks about teachers or other pupils
- general disruption to learning caused by pupils accessing phones in lessons

- pupils phoning parents immediately following an incident so that the ability of staff to deal with an incident is compromised
- publishing photographs of vulnerable pupils, who may be on a child protection plan, where this may put them at additional risk.

Dealing with Breaches

Misuse of the mobile phone will be dealt with using the same principles set out in the school behaviour policy, with the response being proportionate to the severity of the misuse.
Pupils are aware that serious misuse may lead to the confiscation of their mobile phone for up to a term, communication with parents and the imposition of other sanctions up to and including exclusion from school. If the offence is serious it will be reported to the Police.

Rules for the Acceptable Use of a Mobile Phone in School by Pupils

Pupils are strongly discouraged from bringing mobile phones into school. If they choose to do so it is on the understanding that they agree with the following limitations on its use, namely:

- Mobile phones must be switched off and placed in a bag or locker on arrival.
- **The phone must be kept out of sight and not used in the building and school grounds.**
- No pupil may take a mobile phone into a room or other area where examinations are being held.
- The security of phone will remain the pupil's responsibility.
- If asked to do so, content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher

Unacceptable use

The school will consider any of the following to be unacceptable use of the mobile phone and a serious breach of the school's behaviour policy resulting in sanctions being taken.

- Photographing or filming staff or other pupils without their knowledge or permission
- Photographing or filming in toilets, changing rooms and similar areas
- Bullying, harassing or intimidating staff or pupils by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites
- Refusing to switch a phone off or handing over the phone at the request of a member of staff

- Using the mobile phone outside school hours to intimidate or upset staff and pupils will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time
- Using a mobile phone outside school hours in such a way that it undermines the stability of the school and compromises its ability to fulfil the stated aim of providing 'a clear moral and ethical lead'.

Sanctions

Pupils and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines, following the schools behaviour policy.
In addition:

- Pupils and their parents should be very clear that the school is within its rights to **confiscate the phone for up to a term** where the guidelines have been breached.
- Using the mobile phone outside school hours to intimidate or upset staff and pupils or undermine the stability of the school in any way will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.
- **If a phone is confiscated, school will make it clear for how long this will be and the procedure to be followed for its return.**
- Pupils should be aware that the police will be informed if there is a serious misuse of the mobile phone where criminal activity is suspected.
- If a pupil commits an act which causes serious harassment, alarm or distress to another pupil or member of staff the ultimate sanction may be permanent exclusion. School will consider the impact on the victim of the act in deciding the sanction.

Confiscation Procedure

If a mobile phone is confiscated then:

- the pupil will be informed that the phone can be collected at the end of school day *from the Head or nominated senior member of staff.*
- the confiscation will be recorded in the school behaviour log on ISAMS for monitoring purposes
- school will ensure that confiscated equipment is stored in such a way that it is returned to the correct person.

- in the case of repeated or serious misuse the phone will only be returned to a parent/carer who will be required to visit the school by appointment to collect the phone. This may be at the end of a week, a half term or longer. At the discretion of the Head the phone may be returned to the pupil at the end of the confiscation period.

- where a pupil persistently breaches the expectations, following a clear warning, the Head may impose an outright ban from bringing a mobile phone to school. This may be a fixed period or permanent ban.

Where the Phone has been used for an Unacceptable Purpose

The Head or a designated staff member will ask to view files stored in confiscated equipment and if necessary seek the cooperation of parents in deleting any files which are in clear breach of these guidelines unless they are being preserved as evidence. If required evidence of the offence or suspected offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen School will consider whether an incident should be reported to the safeguarding Governor. The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator or the victim which needs further investigation.

Parents' Use of Mobile Phones on School Site

Parents are not allowed to use their mobile phones or their camera facility whilst in the school building or site. School policy on this matter will be explained to parents and placed on the school website.
During group outings nominated staff will have access to a school mobile or IPAD which may be used for photographs or for contact purposes.
In the case of school productions parents / carers are permitted to take pictures of their own children in accordance with school protocols which strongly advise against the publication of any such photographs on social networking sites.

Staff use of Personal Devices

Staff are not permitted to use their own mobile phones or devices for contacting pupils, young people or those connected with the family of the pupil. Staff will be issued with a school phone where contact with pupils, parents is required, for example a mobile on school trips or staff based landline in departments or school offices.

- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode and not used during teaching periods unless in emergency circumstances. They **MUST BE OUT OF SIGHT** in classrooms and the school building.

- Staff should use mobile phones in designated areas such as the staff room away from children**; not in open areas and within view of children regardless of the time of day.**
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.
- Staff use of mobile phones during the school day will be limited to the morning break, lunch break and after school.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Staff should not send and receive texts in classrooms or use camera phones at any time.
- Staff should never contact pupils from their personal mobile phone, or give their mobile phone number to pupils. If a member of staff needs to make telephone contact with a parent, a school telephone should be used.
- Staff should never store parents' or pupils' telephone or contact details on their mobile phone, as this allows the possibility of inappropriate contact.
- Staff should never send, or accept from anyone, texts or images that could be viewed as inappropriate.
- If a member of staff suspects a message, text or similar may contain inappropriate content it should not be opened but a senior member of staff, preferably the online safety coordinator or DSL should be contacted.

Created and Reviewed by : Dawn Akyurek April 2018	**Policy Category:** Mandatory Group Policy
Approved by : Elena Benito & KGB April 2018	**Last Review:** June 2019
Approved by KGB:	**Reviewed by:** Martin Glynn and Luke Tamblyn June 2021

Appendix 1 - Guidance on Confiscation

DfE guide on screening and searching - What the law allows
(n.b. this guidance is currently under review)

Please be aware that the searching of mobile phones and requesting of pin codes is illegal in some countries. Always attempt to get the student to volunteer the information or have a parent present.

"Schools' general power to discipline, as set out in Section 91 of the Education and Inspections Act 2006, enables a member of staff to confiscate, retain or dispose of a pupil's property as a disciplinary penalty, where reasonable to do so."
See below for full document
http://www.education.gov.uk/schools/pupilsupport/behaviour/f0076897/screening
DfE Behaviour and discipline guidance for school staff
http://media.education.gov.uk/assets/files/pdf/b/behaviour%20and%20discipline%20in%20schools%20%20%20guidance%20for%20teachers%20and%20school%20staff.pdf

Appendix 2 - Legal Context

Common Offences Related to the Misuse of Mobile Telephones
The key to both offences below is that the message/picture/video is actually **SENT .** (If it is only stored on a device the offence is not complete.)

1. Malicious Communications Act 1988
It is an offence to send an indecent, grossly offensive or threatening letter, electronic communication or other article to another person with the intention that it should cause them distress or anxiety
2. Communications Act 2003
Section 127 covers all forms of public communications

127(1) a person is guilty of an offence if they-
a) send by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
(b) causes any such message or matter to be so sent.

127(2) A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, they –
(a) send by means of a **public** electronic communications network, a message that they know to be false,
(b) causes such a message to be sent; or
(c) persistently makes use of a public electronic communications network

Appendix 3 – Sources of Help

Resources
Resources are available to support teachers, parents and pupils to promote the safe use of mobile phones and other technologies both in school and at home. Below is a note of the resources available and a short description of what each one contains. These resources have been drawn from a variety of sources, including the Mobile Network Organisations.

The **O2 Nuisance Call Bureau** provide practical help and advice to schools – whether they're having serious problems relating to bullying on mobile phones, nuisance calls or texts, happy slapping, or any other issues. Further information is available from http://protectourchildren.o2.co.uk/AdviceForSchools.jsp

Mobile phone guide for parents from Orange
http://www1.orange.co.uk/safety/images/guide_for_parents.pdf

Orange Educational resources on the safe and secure uses of mobile phones, and access to the "Incoming message" video and support materials http://www1.orange.co.uk/about/corporateresponsibility/quicklinks/educational_resources.html

Orange
http://www.orange.co.uk/communicate/safety/

Mobile Network Operators and Regulators
http://protectourchildren.o2.co.uk/PreventBullying.jsp

T-Mobile
http://www.t-mobile.co.uk/personal/pages.do/corpinfo/about-tmobile/corporate-responsibility/landing

For pupils
Newsround article on happy slapping including advice for pupils on what to do if it happens to them
http://news.bbc.co.uk/cbbcnews/hi/newsid_4490000/newsid_4498700/4498719.stm

respect*me* 's cyberbullying resource page:
http://www.respectme.org.uk/What-is-Cyberbullying.html

Cybermentors
http://cybermentors.org.uk/

Childline
http://www.childline.org.uk/

For parents/carers
Mobile phones: What parents need to know provides help and advice about modern mobile phones for families and carers. http://www1.orange.co.uk/documents/regulatory_affairs/guide_for_parents.pdf

Child Exploitation and Online Protection Centre
http://www.ceop.police.uk/

Appendix 4

Safeguarding concerns which may be raised by mobile phone use in school
Child sexual exploitation (CSE)
A feature of some of the recent cases where teenage girls have been groomed for sex has been giving them expensive phones as a gift. The unexpected acquisition of an expensive mobile phone by girls who are unlikely to be able to afford one themselves should trigger a safeguarding concern.
The same approach is often used to draw children into selling drugs.

King's College
The British School of Madrid
Soto de Viñuelas

Appendix A5:

Sexting in schools policy: Youth Produced Sexual Imagery and How to Handle It

Contents

1.0 SECTION ONE – BACKGROUND AND CONTEXT

1. 1 Who is this guidance for?

This guidance is for designated safeguarding leads, Headteachers and senior leadership teams within the group.

1.2 What does this guidance cover?

This guidance covers:

- Responding to disclosures
- Handling devices and imagery
- Risk assessing situations
- Involving other agencies, including escalation to the police
- Recording incidents
- Involving parents
- Preventative education

1.3 What is the status of this guidance?

This guidance has been produced by the UK Council for Child Internet Safety (UKCCIS) Education Group in parallel with guidance for policing from the National Police Chiefs Council (NPCC).

The UKCCIS Education Group is chaired by CEOP, with representatives from the Department for Education, the NSPCC, Barnardo's, the UK Safer Internet Centre, Childnet, the PSHE Association, Parent Zone, Kent County Council and the National Education Network.

A wide range of other schools, local authorities, police forces and organisations have also been consulted including Ofsted, the Disclosure and Barring Service, the Home Office and the Internet Watch Foundation.

This guidance replaces 'Sexting in Schools: What to do and how to handle it.'

This guidance is non-statutory and is supplementary to the Keeping Children Safe in Education statutory guidance and complements the Searching, Screening and Confiscation guidance at school.

1.4 Definitions

This guidance replaces 'Sexting in Schools: What to do and how to handle it.' and introduces the phrase 'youth produced sexual imagery.' This is to ensure clarity about the issues this guidance addresses.

Whilst professionals refer to the issue of 'sexting' there is no clear definition of 'sexting'. Many professionals consider sexting to be 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the Internet.'[1] Yet when children and young people are asked 'What does sexting mean to you?' they are more likely to interpret sexting as 'writing and sharing explicit messages with people they know'[2]. Similarly, the majority of parents think of sexting as flirty or sexual text messages rather than images.[3]

Regardless of what you call this practice, the greatest risks tend to arise when young people share sexual photos or videos. Sharing sexual photos and videos of under 18s is also illegal and therefore causes the greatest complexity for schools and other agencies when responding.

This guidance has been produced to help schools respond to 'youth produced sexual imagery.' This best describes the practice because:

- 'Youth produced' includes young people sharing images that they or another youth has created of themselves
- 'Sexual' is clearer than 'indecent.' A judgement of whether something is 'decent' is both a value judgement and dependent on context.
- 'Imagery' covers both still photos and moving videos

The types of incidents which this guidance covers are:

- A person under the age of 18 creates and shares a sexual photo or video of themselves and shares it with a peer under the age of 18
- A person under the age of 18 shares a sexual photo or video created by another person under the age of 18
- A person under the age of 18 is in possession of a sexual photo or video created by another person under the age of 18

[1] Adolescents and self-taken sexual images - Cooper, Quayle, Jonsson, Svedin, 2014
[2] I wasn't sure it was normal to watch it. NSPCC, Middlesex University, Office of the Children's Commissioner 2016
[3] Childline Sexting Survey 2016

- A person under the age of 18 creates and shares a sexual photo of themselves and shares it with someone over the age of 18

This guidance does not cover the sharing of sexual photos of people under 18 by adults as this constitutes child sexual abuse.

1.5 Why have we produced this guidance?

Sharing photos and videos online is part of daily life for many people, enabling them to share their experiences, connect with friends and record their lives.

Photos and videos can be shared as text messages, email, posted on social media or increasingly via mobile messaging apps, such as SnapChat, WhatsApp or Facebook Messenger.

90% of 16-24 year olds and 69% of 12-15 year olds own a smartphone[4], giving them the ability to quickly and easily create and share photos and videos.

This increase in the speed and ease of sharing imagery has brought concerns about young people producing sexual photos and videos of themselves and sharing them. This can expose them to risks, particularly if the imagery is shared further, including embarrassment, bullying and increased vulnerability to sexual exploitation. Producing and sharing sexual images of under 18s is also illegal.

Although the taking of such imagery will likely take place outside of school, these issues will often manifest in schools and organisations working with children and young people. Schools and other organisations need to be able to respond swiftly and confidently to ensure that children are safeguarded, supported and educated.

This guidance aims to support schools in developing procedures to respond to incidents involving 'youth produced sexual imagery.' It also signposts sources of resources and support.

These procedures should be part of a school's safeguarding arrangements and all incidents of youth produced sexual imagery should be dealt with as safeguarding concerns.

[4] http://media.ofcom.org.uk/news/2015/cmr-uk-2015/
stakeholders.ofcom.org.uk/binaries/research/media-literacy/children-parents-nov-15/charts_section_3.pdf

The response to these incidents should be guided by the principle of proportionality. The primary concern should be the welfare and protection of the young people involved.

1.6 How much is this really happening?

'Parents expect you to be involved in sexting even when you are not.' Simone, 14

Most young aren't sharing sexual imagery of themselves[5].

A 2016 NSPCC / Children's Commissioner study found that one in ten boys and girls had taken topless pictures of themselves and 3% had taken fully naked pictures. Of those who had taken sexual images, 55% had shared them with others. A simple extrapolation of these figures against current population estimates would suggest that around 110,000 children aged 13-17 have taken fully naked pictures of themselves and around 61,000 shared them.

Although most young people aren't sharing this type of imagery, the potential risks are significant. As a result concerns about this issue in schools remain high. Research conducted by 'the key' discovered that 61% of its secondary school head teacher members reported 'sexting' as a concern. This placed it higher than drugs, obesity and offline bullying in terms of frequency of reporting as a concern.[6]

2.0 The law

Much of the complexity of responding to youth produced sexual imagery is due to its legal status. 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.

The relevant legislation is contained in the Protection of Children Act 1978 (England and Wales) as amended in the Sexual Offences Act 2003 (England and Wales).

Specifically:

- It is an offence to possess, distribute, show and make indecent images of children.
- The Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18.

[5] I wasn't sure it was normal to watch it. NSPCC, Middlesex University, Office of the Children's Commissioner 2016

[6] https://www.thekeysupport.com/media/filer_public/08/32/0832cb2c-85c1-4ed4-891d-4a106d3c72b1/summer_report_2015_school_leaders_concerns_about_pupil_wellbeing.pdf

'Indecent' is not defined in legislation. When cases are prosecuted, whether any photograph of a child is indecent is for a jury, magistrate or District Judge to decide based on what is the recognised standard of propriety[7]. For most purposes, if imagery contains a naked young person, a topless girl, displays genitals or sex acts, including masturbation, then it will be indecent. Indecent images may also include overtly sexual images of young people in their underwear.

2.1 Criminalisation of children

The law criminalising indecent images of children was created long before mass adoption of the internet, mobiles and digital photography. It was also created to protect children and young people from adults looking to sexually abuse them or gain pleasure from their sexual abuse. It was not intended to criminalise children.

Despite this, young people who share sexual imagery of themselves, or peers, are breaking the law.

We should not, however, unnecessarily criminalise children and young people. Children with a criminal record face stigma and discrimination in accessing education, training, employment, travel and housing and these obstacles can follow a child into adulthood[8]

Whilst young people creating and sharing sexual imagery can be very risky, it is often the result of young people's natural curiosity about sex and their exploration of relationships. Often, young people need education, support or safeguarding, not criminalisation.

2.2 The police response

Schools need to feel confident that they can seek advice and involvement of the police and that young people will not be criminalised as a result.

The National Police Chiefs Council (NPCC) in the UK is clear that incidents involving youth produced sexual imagery should primarily be treated as safeguarding issues.

[7] http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/
[8] Growing Up, Moving On – The International Treatment of Childhood Criminal records, Standing Committee on Youth Justice, 2016

The police may need to be involved in cases to ensure thorough investigation and there are incidents, highlighted in this guidance, which should always be referred to the police. However, it would only be in cases where evidence is uncovered that a young person is knowingly engaging in coercive, threatening or exploitative behaviour, that a criminal justice response and formal sanction against a young person would be considered proportionate and applied. In the absence of evidence of this, cases should not result in any form of criminal justice sanction (i.e. the young person being charged or given a youth caution).

The new NPCC guidance, produced in parallel to this guidance, outlines what a proportionate response to youth produced sexual imagery looks like and should ensure that there is greater consistency across each police service in England and Wales. A copy of the guidance can be found **here.**

2.3 Crime recording

Where the police are involved in incidents of youth produced sexual imagery they are obliged, under the Home Office Counting rules and National Crime Recording Standards, to record the incident on their crime systems. The incident will be listed as a 'crime' and the young person involved will be listed as a 'suspect.'

This is not the same as having a criminal record.

However, there have been concerns that young people could be negatively affected should that crime be disclosed, for example, on an enhanced Disclosure and Barring Service (DBS) check.

To mitigate this risk, the NPCC have worked with the Home Office and the Disclosure and Barring Service and provided policing with a new way of recording the outcome of an investigation into youth produced sexual imagery. This is called Outcome 21.

2.4 Outcome 21

Every 'crime' recorded on police systems has to be assigned an outcome from a predefined list of outcome codes. As of January 2016 the Home Office launched a new outcome code (outcome 21) to help formalise the discretion available to the police when handling crimes such as youth produced sexualised imagery.

Outcome 21 states:

> *Further investigation, resulting from the crime report, which could provide evidence sufficient to support formal action being taken against the suspect is not in the public interest. This is a police decision.*

This means that even though a young person has broken the law and the police could provide evidence that they have done so, the police can record that they chose not to take further action as it was not in the public interest. The new NPCC guidance outlines how outcome 21 should be applied in cases of youth produced sexual imagery, ensuring that safeguarding is the primary consideration and avoiding the unnecessary criminalisation of children accordingly.

2.5 DBS certificates

A decision to disclose information on a DBS certificate is made on the basis of whether that information is relevant to the risk an individual might pose to children, young people or vulnerable adults.

The Home Office, NPCC Lead for Disclosure and the Disclosure and Barring Service (DBS) have made amendments to guidance to ensure that officers making disclosure decisions are aware of outcome 21 and its application in incidents of youth produced sexual imagery. Officers will be aware that if police have applied outcome 21 then this will have been on the grounds that it was not proportionate to pursue a criminal justice outcome or formal sanction in this case.

Disclosure of an incident of youth produced sexual imagery with outcome 21 on a DBS certificate would therefore be unlikely.

An incident would only be disclosed if other information indicated that the individual posed a risk, for example, they had committed other relevant offences or the youth produced sexual imagery appeared to form part of a pattern of offending.

Consequently, schools can be confident that the police have discretion to respond appropriately in cases of youth produced sexual imagery and to record incidents in a way which will not have a long term negative impact on young people.

3.0 SECTION TWO – HANDLING INCIDENTS

3.1 Initial response

All incidents involving youth produced sexual imagery should be responded to in line with the school's safeguarding and child protection policy.

Keeping children safe in education statutory guidance sets out that all schools should have an effective child protection policy. Youth produced sexual imagery and your school's approach to is reflected in our policy..

When an incident involving youth produced sexual imagery comes to a school's attention:

- The incident should be referred to the Designated Safeguarding Lead as soon as possible.
- There should be an initial review meeting with the safeguarding team and a subsequent interview with the children involved. At that meeting there needs to be a clear record taken of the incident with dates, timings and names in accordance with safeguarding protocols.
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the child at risk of harm.

3.2 Disclosure by pupils

Disclosures about youth produced sexual imagery can happen in a variety of ways. The pupil affected may inform a class teacher, the safeguarding lead in school, or any member of the school staff. They may report through an existing reporting structure, or a friend or parent may inform someone in school or the police directly.

All members of staff must be made aware of how to recognise and refer any disclosures of incidents involving youth produced sexual imagery. This should be covered within staff training and within your school safeguarding policies and procedures.

Any direct disclosure by a young person should be taken very seriously. A young person who discloses they are the subject of sexual imagery is likely to be embarrassed and worried about the consequences. It is likely that disclosure in school was a last resort and they may have already tried to resolve the issue themselves.

3.3 Initial review meeting

The initial review meeting with the safeguarding team should aim to establish:

- Whether there is an immediate risk to a pupil or pupils
- If a referral should be made to the police or social care
- If you need to view the imagery in order to safeguard the child, – in most cases, you should not view imagery
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and on what platforms
- If there is a need to contact another school, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases, yes

An immediate referral to police or social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a child has been coerced or blackmailed
3. What you know about the imagery suggests the content is extreme or violent
4. A pupil involved has been identified as vulnerable, previously been abused, or is currently involved with social care
5. The imagery involves sexual acts and any pupil in the imagery is under 13
6. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery

If none of the above apply you may decide to respond to the incident as a school without involving other agencies.

The decision to respond to the incident without involving other agencies would be made in cases when a Designated Safeguarding Lead is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework.

The decision should be made by the school's Designated Safeguarding Lead, Headteacher and with additional input from other members of staff if appropriate.

The decision should be in line with the group's child protection procedures and should be based on consideration of the best interests of the pupils involved. This should take into account proportionality as well as the welfare and protection of the young people.

Most incidents that are dealt with by the school directly would be those where a young person has shared imagery consensually in a romantic relationship or as a joke and where there is no intended malice. In contrast any incidents with aggravating factors, for example, a young person sharing someone else's imagery without consent and with malicious intent, should be referred to police and/or social care.

3.4 Assessing the risks

The circumstances of incidents can vary widely. If at the initial stage you have decided not to refer to police and or social care the Designated Safeguarding Lead should conduct a further review to establish the facts so you can assess the risks and effectively manage the incident.

When assessing the risks the following themes should be considered:

- How the image was generated? Why it was generated? Was the child coerced or put under pressure to produce the imagery?
- Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
- What is the impact on the pupils involved?
- Do the pupils involved have additional vulnerabilities?

Designated safeguarding leads should always use their professional judgement in conjunction with their colleagues to assess the incidents. To complement and support your professional judgment you will find a list of questions which you should consider at Annex A

3.5 Informing parents

Parents should be informed and involved in the process at an early stage unless through your risk assessment you have determined that the child might be put at further risk from a parent or carer. In the initial investigation phase you will want to inform parents and invite them to come into school to discuss the incident

You will also need to notify parents if you are informing the police or removing a device from a child and the reason for doing so.

Annex B contains further advice and information about involving parents and carers.

3.6 Involving other agencies

Following the risk assessment you may need to involve other agencies in the handling of the incident. Other agencies can be involved in different ways.

The police may need to be involved if the incident is of a serious nature, you may need additional support or need to make a referral to social care or your local Multi Agency Hub (MASH) or you may need support for a young person from organisations like the NSPCC (Childline), Brook, Barnardos or CAMHS. Decisions on whether to involve other agencies should always involve the designated safeguarding lead.

3.7 Reporting incidents to the police

If it is necessary to refer to the police, contact should be made through your existing arrangements. This may through your safer schools officer, a PCSO, your local neighbourhood police or by dialling 101.

Once a report is made to the police, the report has to be recorded and the police will conduct an investigation. This may include seizure of devices and interviews with the children involved. The police guidance that has been developed in parallel with this guidance gives further detail on what will happen once an incident is referred onto the police.

Things to be aware of when making reports to the police:

Be aware that the police are not able to offer general advice on incidents. If you name the children involved / specifics they are duty bound to record and investigate all criminal activity reported.

If you are making a report through the 101 service, be aware that the person answering the call is a call handler and deals with a wide variety of crimes.

If you have Safer Schools Officers in your area they will be able to offer direct support to schools on prevention and management of incidents

3.8 Securing and handing over devices to the police

If a device needs to be seized and passed onto the police then the device(s) should be confiscated from a student and the police should be called. The phone should be turned off and placed under lock and key until the police are able to come and retrieve it.

If seizure is required and a child refuses to hand over their device, the parents should be informed and police potentially contacted.

4.0 Social care contact and referrals

If the Designated Safeguarding Lead is aware that children's social care are currently involved with a pupil involved in an incident of youth produced sexual imagery then they must contact Children's Social Care to inform them of the incident. You should also contact Children's Social Care if you believe they may be involved, or have been involved with a child in the past.

If as a result of your investigation you believe there are wider issues which meet the threshold for social care involvement then you should make a referral in line with your child protection procedures.

All schools should have an initial point of contact with their local authority which can help you make effective decisions about the handling of incidents and the best referral pathways for children.

Many Local Safeguarding Children Boards (LSCBs) will have published procedures to enable professionals to respond to a range of safeguarding concerns which may relate to youth produced sexual imagery, including (but not limited to) harmful behaviours and underage sexual activity. Most LSCB's have thresholds which they publish in their areas. Designated safeguarding leads should ensure that are familiar with any relevant documents and guidance.

5.0 Searching devices, viewing and deleting imagery

5.1 Should you view the image or video?

You should **not** view youth produced sexual images or videos unless there is good reason to do so. Wherever possible you should make decisions based on what you have been told about the content of the imagery.

The decision to view imagery would be based on your professional judgement as Designated Safeguarding Lead and you should ALWAYS comply with your safeguarding and child protection policy and procedures. You should never view imagery if the act of viewing it will cause significant distress or harm to the pupil.

If you decide to view the imagery you would need to be satisfied that viewing:

- is the only way to make a decision about whether to involve other agencies (ie you are not able to establish the facts from the pupil(s) involved)
- is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the child or parent in making a report
- is unavoidable because a pupil has presented an image directly to a staff member or the imagery has been found on a school device or network

If it is necessary to view the image(s) then you must:

- Never copy, print or share the imagery. This is illegal.
- Inform the headteacher of your decision to view the imagery and the reasons why
- Ensure viewing is only undertaken by one member of staff. This should be the designated safeguarding lead or another member of the safeguarding team with delegated authority from the headteacher.
- Ensure images are viewed by a staff member of the same sex as the pupil in the imagery
- Record the fact that you viewed the imagery in your safeguarding records including who was present, why the image was viewed and any subsequent actions. Ensure this is signed and dated and meets the wider standards set out by Ofsted for recording safeguarding incidents.

Further details on searching, deleting and confiscating devices can be found on the DfE web site in the *Searching, Screening and Confiscation* advice.

5.2 Deletion of images

If you have decided that police do not need to be involved, then you will need to manage the deletion and removal of imagery from devices, online storage and social media sites.

The *Searching, Screening and Confiscation advice* highlights that schools have the power to search pupils for devices, search data on devices and delete youth produced sexual imagery this is not the case in Spain where teachers are not able to search or view the imagery on the phone..In this case the parents must be called and informed.

However, just as in most circumstances it is not recommended that teachers view imagery, you should also not search through devices and delete imagery unless there is good reason to do so.

It is recommended that pupils are asked to delete imagery and to confirm that they have deleted the imagery. Pupils should be given a deadline for deletion across all devices, online storage or social media sites.

Pupils should be informed that if they refuse or it is later discovered they did not delete the image they are committing a criminal offence and the police may become involved. All of these decisions need to be recorded, including times, dates and reasons for decisions made and logged in the safeguarding records. Parents and carers should also be informed unless this presents a further risk to the child.

At this point schools may want to invoke their own disciplinary measures to discourage students from sharing, generating or receiving images but this is at the discretion of the school and should be in line with its own behaviour policies.

You should note that if your school does intend to use the power to search for devices then your mobile phone policy needs to clearly articulate that devices can be searched, confiscated and imagery deleted if they contain youth produced sexual imagery unless this breaks the law of the country. You should highlight why this is important, the conditions in which you will view images and the sanctions that are likely to be imposed if imagery of this nature is found

6.0 Interviewing and talking to the child/children involved

Once you have assessed that the child or young person is not at immediate risk, it may be necessary to have a conversation with the student and decide the best course of action. If possible, the Designated Safeguarding Lead should carry out this this conversation. However, if the child feels more comfortable talking to a different teacher, this should be facilitated where possible. If the child prefers, this initial conversation may be carried out without their parents present, if the school's policies allow this. However if after the initial conversation it transpires that there are safeguarding or welfare concerns then the parents should be informed, unless informing them will place the child at further risk. Within the meeting there needs to be a clear record taken of the incident with dates, timings and names in accordance with safeguarding protocols, and the child needs to be made aware that this will happen.

- When discussing the sharing of youth-produced sexual imagery, it is important that the Designated Safeguarding Lead: Recognises the pressures that young people are under to take part in sexting and, if relevant, supports the student's parents to understand the wider issues and motivations around sexting.
- Remains solution focused and avoids questions such as 'why have you done this?' which may prevent the young person from talking about what has happened.
- Reassures the young person that they are not alone and will do everything that they can to help and support them.
- Helps the young person to understand what has happened by discussing the wider pressures that they may face and the motivations of the person that sent on the photo.
- Discusses issues of consent and trust within healthy relationships. Explain that it is not ok for someone to make them feel uncomfortable, to pressure them into doing things that they don't want to do, or to show them things that they are unhappy about. Let them know that they can speak to you if this ever happens.

The purpose of the conversation is to:

- Identify, **without looking**, what the image contains and whether anyone else has been involved.
- Find out who has seen or shared the image and how further distribution can be prevented.

7.0 Recording incidents

All incidents relating to youth produced sexual imagery need to be recorded in school. This includes incidents that have been referred to external agencies and those that have not.

Ofsted highlight that when inspecting schools in relation to safeguarding they will be looking for the following:

- Are records up to date and complete?
- Do records demonstrate both effective identification and management of the risk of harm?
- Do records demonstrate sound decision-making, appropriate responses to concerns and evidence of relevant referrals made in a timely manner?
- Do they indicate that appropriate action is taken in response to concerns and allegations in a timely manner?
- Do they show evidence of tenacity in following up concerns with relevant agencies?
- Do they provide evidence of effective partnership working and sharing of information?
- Is there evidence of attendance at or contribution to inter-agency meetings and conferences?
- Is there clarity about the school's policy relating to the sharing of information internally, safe keeping of records, and transfer when a pupil leaves the school?

In cases that relate to youth produced sexual imagery it is important that schools reflect all of the areas above when they are recording incidents.

In addition, where schools do not refer incidents out to police or social care they should record their reason for doing so and ensure that this is appropriately signed off by the Headteacher in school.

8.0 Reporting youth produced sexual imagery online

Children and young people may need help and support in the removal of content (imagery and videos) from devices and social media, especially if they are distressed. Most providers offer a reporting function for account holders and some offer a public reporting function to enable a third party to make a report on behalf of the child.

- The quickest way to get content removed from the internet is for the person who posted it to take it down. If the child posted the content themselves using their account, ask them to log in and delete it.
- If someone else posted the image or re-posted it, ask them to log in and delete it from any sites they've shared it on.
- If you don't know who has posted it, or the poster refuses to take it down, you can still report the content and if it breaches a site's Terms of Service then it will be removed.

You should act especially quickly to remove content containing the following:

- Nudity or suggestive poses.
- Details which might identify a child – for example a school uniform.
- Details which might identify or embarrass other children.

Each provider will have a different approach to dealing with requests for the removal of content and the speed of response. You can find out more by visiting the individual provider's site where they should make public their Terms of Service and process for reporting. Nudity and sexual content is not allowed by the majority of the main providers'. Where this is the case, it should not be difficult to report this content for removal.

The NSPCC's Netaware website provides an overview of the main providers and links to their reporting functions www.net-aware.org.uk

Annex C outlines how to report to some of the major providers and what to do when a site does not have a reporting function.

9.0 Section 3 – Educational responses

9.1 Annex A

When deciding whether to involve other agencies, consideration should be given to the following questions. Answering these questions will help the Designated Safeguarding Lead and the safeguarding team decide whether additional information or support is needed from other agencies or if the school can manage the risk of harm and support the pupils itself.

Why was the imagery shared? Was it consensual or was the pupil put under pressure or coerced?

Why this question?	Young people's motivations for sharing sexual imagery include flirting, developing trust in a romantic relationship, seeking attention or as a joke. Though there are clearly risks when young people share imagery consensually, young people who have been pressured to share imagery are more likely to report negative consequences. A referral should be made to the police if a child has been pressured or coerced into sharing an image, or imagery is being shared without consent and with malicious intent. You should take disciplinary action against pupils who pressure or coerce others into sharing sexual imagery

Has the imagery been shared beyond its intended recipient? Was it shared without the consent of pupil who produced the imagery?

Why this question?	The imagery may have been shared initially with consent but then passed on to others. A pupil may have shared the image further with malicious intent, or they may not have had a full understanding of the potential consequences. The police should be informed if there was a deliberate intent to cause harm by sharing the imagery or if the imagery has been used to bully or blackmail a pupil.

Has the imagery been shared on social media or anywhere else online? If so, what steps have been taken to contain the spread of the imagery?

Why this question?	If the image has been shared widely on social media, this could cause significant embarrassment for the pupil and have a long term impact on their online reputation. It could also increase the risk of them being bullied or contacted by strangers online. You should support a young person to report the imagery to any sites it is hosted on. You can find information on reporting in Annex B. If the child has tried to report the imagery and it has not been removed you should contact ChildLine or the Professionals Online Safety Helpline. If the child is being contacted by people they don't know who have viewed the image then you should report to CEOP.

How old is the pupil or pupils involved?

Why this question?	Children under the age of 13 are unable to consent to sexual activity. Any imagery containing sexual activity by under 13s should be referred to the police. Being older can give someone power in a relationship so if there is a significant age difference it may indicate the young person felt under pressure to share. If you believe the imagery contains acts which you would not expect a child of that age to engage in then you should refer to the police. The Brook Traffic Light tool provides guidance on harmful sexual behaviour at different ages.

Did the child send the image to more than one person?

Why this question?	If a pupil is sharing sexual imagery with multiple people this may indicate there are other issues which they need support with. Consideration should given to their motivations for sharing. If you believe there are wider safeguarding concerns then you should mak referral to social care.

Does the pupil understand the possible implications of sharing the image?

Why this question?	Children may produce or share imagery without fully understanding the consequences of what they are doing. They may not, for example, understand how it may put them at risk or cause harm to another pupil. Exploring their understanding may help you plan an appropriate response helping you assess, for example, whether they passed on an image with deliberate intent to harm.

Do you have any concerns about the pupil's vulnerability?

Why this question?	Consideration should be given to whether a pupil's circumstances or background makes them additionally vulnerable. This could include being in care, having special educational needs or disability or having been a victim of abuse. Where there are wider concerns about the care and welfare of a pupil then consideration should be given to referring to children's social care.

Are there additional concerns if the parents or carers are informed?

Why this question?	Parents should be informed of incidents of this nature unless there is good reason to believe that informing them will put the child at risk. This may be due to concerns about parental abuse or cultural or religious factors which would affect how they or their community would respond. If a pupil highlights concerns about involvement of their parents then the Designated Safeguarding Lead should use their professional judgment about whether it is appropriate to involve them and at what stage. If a school chooses not to involve a parent they must clearly record the reasons for not doing so.

9.2 Annex B

Educating parents about sexting:

Parents have a key role to play in helping to inform children about sexting and supporting them to make positive decisions. NSPCC research found that 50% of parents said they would like to receive more information about sexting to support them in talking to their children and understanding healthy relationships. They would prefer to receive this through leaflets, booklets, and newsletters from their child's school or police and through online forums or resources. Information needs to be accessible and easy to read. Resources for parents should include:

- An overview of what sexting is, highlighting in particular that it includes the sending of images and videos
- The pressures, motivations and expectations faced by young people to behave sexually
- Information about consent and trust within healthy relationships.
- The prevalence of sexting – showing that numbers are low but highlighting the vulnerabilities of those who share, particularly to those unknown to them
- Explanation of what the risks associated with sexting are, especially recognising young people's fears/concerns
- Legalities of sexting and naked pictures or videos
- Tips on how parents can support their children if their image has been publicly shared – signposting to relevant agencies and information/resources
- What parents can do to help remove images/empower young people – signposting Childline's partnership with the IWF
- Role of police and schools in incidents – signposting to named roles in each organisation to empower parents to know they are asking the 'right' person

Helping parents when their child has been involved in sexting:

Young people can be involved in sexting in several different ways: they may lose control of their own image; receive an image of someone else; or share an image of another person. It can be difficult for parents whose children have experienced any of these situations to know how to deal with the knowledge that their child has been involved in sexualised activity. Parents may feel shocked, upset, angry, confused, or disappointed.

Whatever their feelings, it is important that professionals listen to their concerns and take them seriously. It can also be helpful for teachers and the police to reassure parents by explaining that it is normal for children to be curious about sex. Below are examples of the advice that police and schools should offer to parents in a range of scenarios:

Parents whose child has lost control of a sexual image should be:

- Advised on the law around sexting, with regards to saving, sharing, or looking at naked or sexual images of children.
- Directed to encourage the young person to delete images from social media accounts, if they have uploaded them themselves.
- Directed to ChildLine's partnership with the Internet Watch Foundation to see if it is possible to get the image removed if it has been shared more widely. This must be done as soon as possible in order to minimise the number of people that have seen the picture. Parents should also be informed about how to report sexual images on individual sites to get them taken down. Or if the image has been shared via a mobile, they should be informed that they can contact the provider in order to get their child's mobile number changed.
- Helped to have conversations with their child in an approachable and supportive way. Parents should be advised to:
  - Reassure the young person that they are not alone and refrain from getting angry. Let them know that you will do everything you can to help.
  - Listen and offer support, rather than criticism
  - Avoid questions, such as 'why have you done this?' which may stop the young person from opening up. Instead stay focused on finding a solution, by asking who the image has been sent to and shared with and agreeing next steps.
  - Help the young person to understand what has happened by discussing the wider pressures that they may face and the motivations of the person that sent on the photo.
  - Discuss issues of consent and trust within healthy relationships. Explain that it is not ok for someone to make them feel uncomfortable, to pressure them into doing things that they don't want to do, or to show them things that they are unhappy about. Let them know that they can speak to you if this ever happens.
- Directed to the child's school if they are concerned that their child is being bullied.
- Directed to services for Harmful Sexual Behaviour, such as the National Clinical Assessment and Treatment Service, if this incident, or similar incidents, have previously occurred.

Parents whose child has been sent a sexual image should be:

- Advised on the law around sexting, with regards to saving, sharing, or looking at naked or sexual images of children.
- Supported to have conversations with their child and advised to:
  - Reassure the young person that they have done the right thing by speaking out and that you are there to help.
  - Explain to the young person the importance of not sharing the image further.
  - Listen to the young person's concerns, without criticising their decisions.
  - Ask whether they requested the photo or if it was unsolicited. Confirm whether it has been sent by an adult or a child.
  - Discuss issues of consent and trust within healthy relationships. Explain that it is not ok for someone to make them feel uncomfortable, to pressure them into doing things that they don't want to do, or to show them things that they are unhappy about. Let them know that they can speak to you if this ever happens.
  - If they asked to receive the photos, explain that they should also not put pressure onto others to do things that they are uncomfortable with.
- Provided with suggested ways that the young person could speak to the sender in order to stop future correspondences. Alternatively, if the young person prefers, informed about how to block the sender.
- Directed to CEOP if the images were shared by an adult or if they are concerned about child exploitation or grooming

Parents whose child has shared another child's image should be:

- Advised on the law around sexting, with regards to saving, sharing, or looking at naked or sexual images of children.
- Supported to have conversations with their child and advised to:
  - Stay calm and refrain from getting angry at the young person.
  - Ask who the image has been sent to and where it has been shared. Agree next steps for taking the image down, including deleting the image from their phone or any social media accounts and reporting it to service providers.
  - Identify whether they asked for the photo or were initially sent it without requesting.
  - Discuss issues of consent and trust in healthy relationships or friendships. Talk about the types of things which are and aren't ok to share and how they would feel if someone shared a personal photo of them. If they have asked for the image, explain the importance of not pressuring others into activities that they may not want to take part in.

- Ask about their motivations for sharing the photo and discuss what they could have done differently. If they have reacted to an upsetting incident, such as the break-up of a relationship, by sending the photo onwards, talk about how they could have managed their feelings in a healthier and more positive way.

- Advised to contact their child's school if they are concerned that their child is behaving in a sexually inappropriate way. They should also be directed to services for Harmful Sexual Behaviour, such as the National Clinical Assessment and Treatment Service, if this incident, or similar incidents, have previously occurred.

All parents whose child has been involved in any of the above should be:

- Advised to contact their child's school, if they have received their child's consent, so that teachers are able to offer support to any student that is affected and ensure that the image is not circulated further.
- Informed about sources of support for their child, in case they are feeling anxious or depressed about what has happened. This can include speaking to a ChildLine counsellor or a GP. If they are concerned that their child is suicidal they should contact 999.
- Provided with information on where they are able to access support themselves if they are concerned or distressed, such as through the NSPCC Helpline.
- Directed to CEOP if they are concerned about child sexual exploitation or grooming.

Resources:

The following resources can be used to support parents and children with sexting. They should be included on school and police websites:

- Children can talk to a ChildLine counsellor 24 hours a day about anything that is worrying them by ringing 0800 11 11 or in an online chat http://www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx
- ChildLine have created Zip-It, which is an app that provides witty comebacks in order to help children say no to requests for naked images https://www.childline.org.uk/Play/GetInvolved/Pages/sexting-zipit-app.aspx
- ChildLine and the Internet Watch Foundation have partnered to help children get sexual or naked images removed from the internet. Children can get their photo removed by talking to a ChildLine counsellor. More information is available here http://www.childline.org.uk/explore/onlinesafety/pages/sexting.aspx

- The NSPCC has information and advice about sexting available on its website- https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/1
- If parents are concerned about their child, they can contact the NSPCC Helpline by ringing 0808 800 5000, by emailing help@nspcc.org.uk, or by texting 88858. They can also ring the Online Safety Helpline by ringing 0808 800 5002.
- CEOP have produced a film resources for parents to help them keep children safe from the risks of sexting. They can be seen here: https://www.thinkuknow.co.uk/Teachers/Nude-Selfies/
- The Safer Internet Centre has produced resources called 'So You Got Naked Online' which help young people to handle incidents of sexting http://childnetsic.s3.amazonaws.com/ufiles/Files%202015/SYGNO%20Booklet%20-%20version%202%20May%202015.pdf

9.3 Annex C

The following provides an overview of the reporting functions provided by the main service providers:

Snapchat

Snapchat offers users the ability to share stories and images/videos. The picture or the 'snap' is shared and then disappears after a few seconds. Snapchat also allows users to share Snapchat Stories these are snaps that are shared in a sequence across a 24 hour period.

Snapchat provides a reporting function here https://support.snapchat.com/en-US/ca/abuse

Users are able to block other users.

WhatsApp

WhatsApp is a messaging service where users can share pictures, texts or videos. These can be shared with one person or multiple users.

WhatsApp does not provide a reporting function.

Users are able to block other users here https://www.whatsapp.com/faq/en/s60/21064391

Instagram

Instagram is a picture and video sharing app which allows users to share images, make comments and post messages.

Instagram provides a reporting function here https://help.instagram.com/443165679053819/

Users are able to block other users.

Facebook

Facebook is a social network which allows users to create a profile, share images, videos and messages.

Facebook provides a reporting function here:

- Social reporting - https://www.facebook.com/help/128548343894719

  This offers users the ability to contact other users directly to ask them to take something down that does not necessarily breach Facebook's terms of service. In some cases the child/young person may not feel comfortable in contacting the person directly so they can use the report flow to use another trusted person to help them – a teacher, friend, parent.

- Public reporting - https://www.facebook.com/help/263149623790594/

  Users who do not have a Facebook account are able to report directly to Facebook using the link above and completing the form.

  Users are able to block other users.

YouTube

YouTube allows users to watch, create and share videos. Users can create their own YouTube account, make a music playlist and create their own channel. Users are also able to comment on other users channels.

YouTube provides a reporting function here https://support.google.com/youtube/answer/2802027

Users can report an individual video, a channel or a comment on a video Please note you need to have an account to be able to report on YouTube.

Google

The "right to be forgotten" ruling allows the public to request the removal of search results that they feel link to outdated or irrelevant information about themselves on a country-by-country basis. Users are able to complete a form to highlight what content they wish to be removed. Users have to specify why the content applies to them and why it is unlawful so the exact URL's relating to the search results need to be referenced. https://support.google.com/legal/contact/lr_eudpa?product=websearch

A list of many other providers and links to their reporting functions can be found at the NSPCC's NetAware website – www.net-aware.org.uk

In the event that a site has no reporting function and if the content is a sexual image you can report it to the Internet Watch Foundation (IWF). Sexual images of anyone under 18 are illegal and the IWF can work to get them removed from sites which do not have reporting procedures. You can report directly to the IWF here **-www.iwf.org.uk**

Support services

If you need additional advice or support in contacting providers, the following organisations may be able to assist:

CEOP – If you are concerned that a child is being sexually abused, exploited or groomed online you should report to CEOP www.ceop.police.uk/safety-centre

The NSPCC adults helpline – 0808 800 5002

The NSPCC have partnered with O2 to offer direct support to parents and other adults on issues relating to online safety.

Childline - https://www.childline.org.uk/Pages/Home.aspx

Childline offers direct support to children and young people including issues relating to the sharing of sexual imagery.

The Professionals Online Safety helpline (POSH) - http://www.saferinternet.org.uk/about/helpline

Tel: 0844 381 4772

The POSH helpline has been set up to support professionals with an online safety concern or an online safety concern for children in their care. Professionals are able to contact the helpline to resolve issues.

Created and Reviewed by : Dawn Akyurek, September 2018	**Reviewed by:** Martin Glynn, June 2021 Luke Tamblyn
Approved by KGB: October 2018	**Next Review:** June 2022