**Name of Policy: Online Safety Policy - safe and appropriate use of the Internet and related technologies**

| | |
|---|---|
| **Author/s:** | Rob Alderman, Mark Rogers and Rory Matthews |
| **Date:** | **September 2021** |
| **Next Review date:** | September 2022 |
| **Links with other policies:** | **Safeguarding, Acceptable Use Policy, Anti Bullying Policy, e-learning policy.** |
| **Links to procedures:** | **Induction for staff and new pupil procedures.** |
| **Approval:** | |

**Woodlands Meed: Building Unique Futures Together**

This includes:

- Providing a safe, secure environment
- Recognising the individual needs and strengths of each child
- Planning and facilitating unique, enjoyable opportunities to maximise learning and potential
- Working with parents/carers and outside agencies to achieve the best for each child
- Ensuring opportunities from the wider community are utilised

**Woodlands Meed Equalities Statement is available on the website: www.woodlandsmeed.co.uk under policies.**

## Overview

### Whole 'school' approach to the safe use of Computing/ICT

Creating a safe Computing/ICT learning environment includes three main elements at Woodlands Meed:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive online safety education programme for pupils, staff and parents.

### Roles, Responsibilities and Acceptable Use

Online safety is recognised as an essential aspect of strategic leadership in Woodlands Meed and the Senior Leadership Team aims to embed safe practices into the culture of

Woodlands Meed. The responsibility for online safety has been delegated to the computing leads in consultation with the IT department, SMT and the Headteacher.

- The Safeguarding lead keeps up to date with online safety issues and ensures the Senior Leadership Team and wider staff are updated as necessary. Staff are reminded / updated about online safety matters as appropriate and in response to specific issues arising.

    - All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following online safety procedures. Safe use of the internet at school and home is discussed in classes.

    - All staff should be familiar with the Acceptable Use and online safety policies and be aware of:

        - Safe use of e-mail.
        - Safe use of Internet including use of internet-based communication services, such as instant messaging and social networking.
        - Safe use of the network, equipment and data.
        - Safe use of digital images and digital technologies, such as mobile phones and digital cameras.
        - Publication of pupil information/photographs and use of websites.
        - Cyberbullying procedures.
        - Their role in providing online safety education for pupils.
        - Their responsibility to report any misconduct or inappropriate use of the internet or related technology amongst colleagues and visitors.

**How will complaints regarding online safety be handled?**

Woodlands Meed will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on internet enabled devices. All instances of inappropriate material appearing on WM technology should be reported to the Safeguarding Team and IT team.

Staff and pupils are given information about infringements of use and possible sanctions.

**Sanctions available include**:

- Interview with Head Teacher or Assistant Head
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- Referral to Local Authority / Police.

**Additional pupil sanctions include:**

- Informing parents /carers
- Rescinding of computer access for given time period.
- Additional supervision using Computing/ICT equipment
- Other sanctions in-keeping with behaviour policy

The Safeguarding Team act as first point of contact for any concern. Any complaint about staff misuse is referred to the Head or Assistant Head.

- Complaints of cyberbullying are dealt with in accordance with the Anti-Bullying Policy.

- Complaints related to child protection are dealt with in accordance with school / Local Authority child protection procedures.

## A. Managing the Internet Safely

**Policy statements:**

Woodlands Meed:

- Maintains broadband connectivity.
- Ensures network health through appropriate anti-virus software and administrates the network to ensure only appropriate programs are in use.
- Ensures removal of access to any website considered inappropriate by staff as soon as possible.
- Uses individual log-ins for pupils and all other users.
- Never sends personal data over the Internet unless it is encrypted or otherwise secured.
- Ensures pupils only publish within appropriately secure online learning environments or other sanctioned cloud based technologies.
- Ensures pupil data available through the school network and stored on our servers (SIMS) is available only to staff with secure passwords.
- Ensures pupils are not permitted to use mobile phones (with or without internet connectivity/cameras) on school premises without specific permission and supervision.
- Ensures data use is in compliance with GDPR regulations.

## B. Policy procedures for teaching and learning

1. **Using the Internet**

Pupils should be encouraged and taught to use the internet to find information or entertainment resources, and trained to search effectively. Awareness should also be raised regarding safe searching, and discussions on reliable and unreliable information online should be regular.

2. **Search Engines**

Some common Internet search options carry risk, and pupils should be taught to use these resources (e.g., image searches) in a safe, appropriate way.

3. **Collaborative Technologies**

There are a number of Internet technologies that make interactive collaborative environments available. Often the terms 'social networking' or 'social media' are used. Examples include blogs (personal web-based diaries or journals), wikis (modifiable collaborative web pages), and podcasting (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). We are also making extensive and increasing use of the Seesaw platform which is accessible to staff, students and families. Using these technologies for activities can be motivational, can develop presentation skills and can help children consider their content and audience. However, they are high risk environments and it is essential that teachers use them carefully.

4. **Video Conferencing**
Webcams and iPads can be used to provide a 'window onto the world' to see what it is like somewhere else. The value of this in terms of seeing activity in otherwise unreachable locations is clear, however staff should always preview websites to ensure that webcam feeds and similar resources are suitable. The highest risks lie with streaming webcams [one-to-one chat / video] that pupils use or access outside of the school environment. Whilst these are rarely used in school, pupils need to be aware of the dangers. Increasingly we use Microsoft teams for meetings and lessons, initially because of changes due to Covid-19 but this is now becoming an embedded part of our practice. Staff should ensure they are never only 1:1 with a student. Wherever possible the session should be recorded although this is not required when there are other staff present virtually or in person.

5. **Social Networking and Messaging Sites**
These are a popular aspect of the web for young people. Sites allow users to share and post web sites, videos, images, etc. It is important for children to understand that these sites are public spaces with adult users. They are environments that should be used with extreme caution. WM blocks such sites, however pupils need to be taught safe behaviour as they may well be able to readily access them outside of school. Pupils should be reminded of the age restrictions for various platforms and that avoiding these can avoid the possibility of some legal protection in the event of a problem.

**6. Podcasts**
Podcasts are essentially audio files published online, often in the form of a radio show, but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables young people to create their own radio broadcast and post this onto the web. Pupils should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments where appropriate.

**7. Chatrooms**
Many sites allow for 'real-time' online chat. Again, pupils should only be given access to educational, moderated chat rooms as appropriate when in school. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school where they may access chatrooms. Many games include in-game chat with other players that can be any area of risk.

**8. Sanctions and infringements**
Woodlands Meed online safety and acceptable use policies need to be made available and explained to staff / governors, and rules should be made clear to pupils and parents. Woodlands Meed has clear possible sanctions for infringements.

Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on computers, the matter should be referred immediately to the Leadership Team and Safeguarding Team. It may be contingent on the content of material that a referral is made to the police. There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence (See section H).

**Policy statements**

- Pupils' use of Computing/ICT will be supervised at all times, as far as is reasonable, and staff will be vigilant regarding pupil use of the internet.

- WM will use a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming and sites of an illegal or inappropriate nature.
- Staff will preview all sites before use and relate concerns over inappropriate sites to the IT team or e-safety co-ordinator.
- Staff will ensure use of the internet is taught at an appropriate level for pupil groups, with an awareness of the risks regarding online safety reinforced regularly.
- Staff will be vigilant when conducting 'raw' image search with pupils eg- Google Images.
- Staff will inform users that Internet use is monitored.
- WM will inform staff and students that they must report any failure of the filtering systems directly to the e-safety co-ordinator/IT Team/SMT.
- WM will use filtering to block all chat rooms and social networking sites except those that are part of an educational network sanctioned by SMT.
- WM will only allow access to approved or checked video sites.
- All staff will sign an acceptable use agreement form and keep a copy on file.
- Students are required by the Seesaw terms of use to have parental permission to use this platform. (https://web.seesaw.me/terms-of-service "*We require that teachers or schools get parental consent before using Seesaw with children who are under the age when they can grant consent on their own.*")
- WM will make clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Staff will challenge instances of cyberbullying in accordance with online safety measures and the bullying policy.
- WM will immediately refer any material we suspect is illegal to the appropriate authorities – Local Authority / Police.

## C. Education programme

1. Establish a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable.
2. Ensure pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the site to the teacher.
3. Ensure pupils and staff know what to do if there is a cyberbullying incident.
4. Establish a clear, progressive online safety education programme throughout all Key Stages, built on national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience. This should include:

    - To STOP and THINK before they CLICK.
    - To understand the risks of using the internet- especially from strangers.
    - To understand how to report abuse
    - To expect a wider range of content, both in level and in audience, than is found in the school library or on TV.
    - To discriminate between fact, fiction and opinion.
    - To develop a range of strategies to validate and verify information before accepting its accuracy.
    - To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what

that may be.

- To know some search engines / web sites that are more likely to bring effective results.
- To know how to narrow down or refine a search.
- To understand how search engines work.
- To understand how photographs can be manipulated.
- To understand appropriate behaviour when using an online environment such as a 'chat' / discussion forum, i.e. no bad language, propositions, or other inappropriate behavior.
- To not download any files – such as music files - without permission.
- To understand that certain files can harm our computers.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos.
- To have strategies for dealing with receipt of inappropriate materials.

5 To ensure that pupils of all abilities have access to and are aware of being safe online. For students with Severe Learning Difficulties to access a curriculum where the Pre-Key Stage statements are clearly highlighted in planning and are made accessible for all learning styles. An increased awareness and understanding of the initial early steps that can trigger early e-safety procedures is vital for all staff.

6. Make advice, guidance and training available to staff and parents, including:

- Information in safety leaflets.
- Suggestions for safe Internet use at home.
- Provision of information about national support sites for parents.

## D: Email safety

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects. However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. Once e-mail is available it is difficult to control its content.

**Policy Statements:**

- E-mail should not be considered private and WM reserves the right to monitor email use.
- The Woodlands Meed Exchange Email system is available for staff to use in school and from home.
- Woodlands Meed does not currently publish individual staff e-mail addresses on the school website, although this may be reconsidered in future for certain staff. Most electronic communications from outside our school community arrive via the school office email.

**Pupils:**

- We only use WM school emails with pupils if sanctioned and relevant to learning.
- Pupils need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate messages. This should be part of the school's online safety and anti-bullying education programme.

- Pupils are introduced to, and use, messaging and e-mail as part of the Computing scheme of work at an appropriate age and level.
- Pupils are taught about appropriate and safe communication when using e-mail.
- Pupils and staff are made aware of the risks in opening attachments.

**Governors**

- Governors will use Woodlands Meed emails in accordance with their code of conduct.

## E: Digital images

**Maintaining a safe school web site**

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work.

Content is submitted by staff then sanctioned by authorised staff before going 'live'.

**Use of still and moving images**

- Pupil images may only appear on the school website if permission to use their photograph online has been granted.
- When showcasing examples of pupils' work use only first names or a year based pseudonym.
- Only use images of pupils in suitable dress to protect the dignity of all pupils.
- Links to any external websites are thoroughly checked before inclusion on website to ensure that the content is appropriate.
- Staff are directed not to use their personal phone or camera without permission e.g. for a school field trip. If personal equipment is being used it should be registered with the school and a clear undertaking given that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.
- Pupils are taught about how images can be abused in their e-safety education programme.
- Permissions for use of pupil photographs are recorded on SIMs for publications and online material.

## F. Cyber Bullying

**Cyber bullying** is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms e.g.

- Sending threatening or abusive text messages or emails, personally or anonymously
- Making insulting comments about someone on a website, social networking site (e.g. Facebook) or online journal (blog)
- Making or sharing derogatory or embarrassing videos/pictures of someone via mobile phone or email.

The use of Computing/ICT to bully could be against the law. Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libelous, may contravene the *Harassment Act 1997 or the Telecommunications Act 1984* for example.

**Responses to cyberbullying**
If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time:

- Advise the child not to respond to the message
- Refer to relevant policies including online safety/acceptable use, anti-bullying and PHSCE and apply appropriate sanctions
- Secure and preserve any evidence
- Inform the sender's e-mail service provider
- Notify parents/carers of the children involved
- Consider informing the police depending on the severity or repetitious nature of offence
- Inform the Local Authority online safety officer
- Inform and request the comments be removed if the site is administered externally
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform police as appropriate.

## G. Use of iPads and tablets

iPads and other mobile learning technologies are an essential part of learning at Woodlands Meed. All pupils across both sites have access to iPads in their classrooms.

**Policy Statements:**

- Woodlands Meed often uses a pupil pledge for pupils to sign (if they are able to) outlining their responsibilities as a user. This is reviewed on a pupil by pupil basis.
- Pupil accounts will not be able to add apps to iPads. All apps will be purchased and allocated by the IT team, in consultation with teaching staff.
- Pupil access to iPads will be monitored in school and use of the internet, as with all web-enabled technology, will be supervised.

## H. Safeguarding concerns and Online Safety matters

**Sexting**
The definition of sexting or 'youth produced sexual imagery' can vary, however for the purposes of this policy sexting is regarded as 'sending or posting sexually suggestive images, including nude or semi-nude photographs or videos, via mobile phones or over the internet. Creating and sharing sexual photos and videos of under 18s is **illegal** and therefore is taken extremely seriously. It also presents a range of risks, which need careful management.

**Handling incidents**
Keeping Children Safe in Education statutory guidance sets out that all schools should have an effective child protection policy. Youth produced sexual imagery and a school's approach to it should be reflected in the policy. All incidents involving youth produced sexual imagery should be responded to in line with the school's safeguarding and child protection policy. When an incident involving youth produced sexual imagery comes to a school or college's attention:

- The incident should be referred to the DSL as soon as possible
- The DSL should hold an initial review meeting with appropriate school staff
- There should be subsequent interviews with the young people involved (if appropriate)
- 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 young person at risk of harm
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

**Disclosure**
Disclosures about youth produced sexual imagery can happen in a variety of ways. The young person affected may inform a class teacher, the DSL in school, or any member of the school or college staff. They may report through an existing reporting structure, or a friend or parent may inform someone in school or college, or inform the police directly. All members of staff (including non-teaching) should 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 the school or college's child protection policy. 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 is a last resort and they may have already tried to resolve the issue themselves.

**Initial review meeting**
The initial review meeting should consider the initial evidence and aim to establish:
• Whether there is an immediate risk to a young person or young people
• If a referral should be made to the police and/or children's social care
• If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
• What further information is required to decide on the best response
• Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
• Whether immediate action should be taken to delete or remove images from devices or online services
• Any relevant facts about the young people involved which would influence risk assessment
• If there is a need to contact another school, college, setting or individual
• Whether to contact parents or carers of the pupils involved - in most cases parents should be involved
An immediate referral to police and/or children's social care should be made if at this initial stage:
**1. The incident involves an adult**
**2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)**
**3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent**
**4. The imagery involves sexual acts and any pupil in the imagery is under 13**
**5. You have reason to believe a pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming**

If none of the above apply then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns become known).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL 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 and if appropriate local network of support.

The decision should be made by the DSL with input from the Headteacher and input from other members of staff if appropriate. The decision should be recorded in line with school policy. The decision should be in line with the school's child protection procedures and should be based on consideration of the best interests of the young people involved. This should take into account proportionality as well as the welfare and protection of the young people. The decision should be reviewed throughout the process of responding to the incident.

**Assessing the risks**

The circumstances of incidents can vary widely. If at the initial review stage a decision has been made not to refer to police and/or children's social care, the DSL should conduct a further review (including an interview with the young people involved) to establish the facts and assess the risks.
When assessing the risks the following should be considered:
• Why was the imagery shared? Was the young person 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?
• Are there any adults involved in the sharing of imagery?
• What is the impact on the pupils involved?
• Do the pupils involved have additional vulnerabilities?
• Does the young person understand consent?
• Has the young person taken part in this kind of activity before?
DSLs should always use their professional judgement in conjunction with their colleagues to assess incidents.

**Informing parents (or carers)**
Parents (or carers) should be informed and involved in the process at an early stage unless informing the parent will put the young person at risk of harm. Any decision not to inform the parents would generally be made in conjunction with other services such as children's social care and/or the police, who would take the lead in deciding when the parents should be informed.
DSLs may work with the young people involved to decide on the best approach for informing parents. In some cases, DSLs may work to support the young people to inform their parents themselves.

**Reporting incidents to the police**
If it is necessary to refer to the police, contact should be made through existing arrangements. This may be through a safer schools officer, a PCSO (Police Community Security Officer), local neighbourhood police or by dialing 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 young people involved.
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 the children involved are named or specifics are provided they are duty-bound to record and investigate all criminal activity reported.
• When making a report through the 101 service, be aware that the person answering the call is a call handler who deals with a wide variety of crimes and may not have specialist knowledge in this area. Ensure any crime reference numbers provided are recorded.
• Safer Schools Officers (where available) are able to offer direct support to schools on prevention and advice on management of incidents.

**Securing and handing over devices to the police**
If any devices need to be seized and passed onto the police then the device(s) should be confiscated and the police should be called. The device should be turned off and placed under lock and key until the police are able to come and retrieve it.

**Children's social care contact and referrals**
If the DSL is aware that children's social care are currently involved with a young person involved in an incident of youth produced sexual imagery then they should contact children's social care. They should also contact children's social care if they believe they may be involved, or have been involved with a young person in the past.
If as a result of the investigation the DSL believes there are wider issues which meet the threshold for children's social care involvement then they should make a referral in line with their child protection procedures.

DSLs should ensure that they are aware of, and familiar with, any relevant local policies, procedures and contact points/names which are available to support schools in responding to youth produced sexual imagery.
If a local area has a Multi-Agency Safeguarding Hub (MASH) then this may be the most appropriate place for schools to initially make a referral.

**Searching devices, viewing and deleting imagery**
Viewing the imagery
Adults should **not** view youth produced sexual imagery unless there is good and clear reason to do so. Wherever possible responses to incidents should be based on what DSLs have been told about the content of the imagery.
The decision to view imagery should be based on the professional judgement of the DSL and should always comply with the child protection policy and procedures of the school or college. Imagery should never be viewed if the act of viewing will cause significant distress or harm to the pupil.

If a decision is made to view imagery the DSL would need to be satisfied that viewing:
• is the only way to make a decision about whether to involve other agencies (i.e. it is not possible to establish the facts from the young people involved)
• is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the young person 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 imagery then the DSL should:
• Never copy, print or share the imagery; this is illegal.
• Discuss the decision with the Headteacher.
• Ensure viewing is undertaken by the DSL or another member of the safeguarding team with delegated authority from the Headteacher.
• Ensure viewing takes place with another member of staff present in the room, ideally the Headteacher or a member of the senior leadership team. This staff member does not need to view the images.
• Wherever possible ensure viewing takes place on school or college premises, ideally in the Headteacher's or a member of the senior leadership team's, office.
• Ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the imagery.
• Record the viewing of the imagery in the school's 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 in **the DfE Searching, Screening and Confiscation advice** (note this advice is for schools only).
If youth produced sexual imagery has been unavoidably viewed by a member of staff either following a disclosure from a young person or as a result of a member of staff undertaking their daily role (such as IT staff monitoring school systems) then DSLs should ensure that the staff member is provided with appropriate support. Viewing youth produced sexual imagery can be distressing for both young people and adults and appropriate emotional support may be required.

**Deletion of images**
If the school has decided that other agencies do not need to be involved, then consideration should be given to deleting imagery from devices and online services to limit any further sharing of the imagery. 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.
*The Education Act 2011 amended the power in* ***the Education Act 1996 to provide that when an electronic device, such as a mobile phone, has been seized, a teacher who has been formally authorised by the headteacher can examine data or files, and delete these, where there is good reason to do so****. This power applies to all schools and there is no need to have parental*

*consent to search through a young person's mobile phone. If during a search a teacher finds material which concerns them and they reasonably suspect the material has been or could be used to cause harm or commit an offence, they can decide whether they should delete the material or retain it as evidence of a criminal offence or a breach of school discipline. They can also decide whether the material is of such seriousness that the police need to be involved.* However, just as in most circumstances it is not recommended that school staff view imagery, it is recommended that schools should not search through devices and delete imagery unless there is good and clear reason to do so.

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

Young people should be reminded that possession of youth produced sexual imagery is illegal. They 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 young person.

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

**Interviewing and talking to the young person/people involved**

Once a school has assessed a young person as not at immediate risk, it may be necessary to have a conversation with them and decide the best course of action. If possible, the DSL should carry out this this conversation. However, if the young person feels more comfortable talking to a different teacher, this should be facilitated where possible.

When discussing the sharing of youth produced sexual imagery, it is important that the DSL:

• Recognises the pressures that young people can be under to take part in sharing such imagery and, if relevant, supports the young person's parents to understand the wider issues and motivations around this.

• Remains solution-focused and avoids questions such as 'why have you done this?' as this may prevent the young person from talking about what has happened.

• Reassures the young person that they are not alone and the school or college 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 imagery.

• 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 the DSL 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.

**Recording incidents**

All incidents relating to youth produced sexual imagery need to be recorded in school or college. 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 look 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 children's social care they should record their reason for doing so and ensure that this is signed off by the Headteacher.

**Reporting youth produced sexual imagery online**
Young people may need help and support with the removal of content (imagery and videos) from devices and social media, especially if they are distressed. Most online service 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 young person.
Refer to sexting in schools and colleges – responding to incidents and safeguarding young people, UK council for child internet safety for further information:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF