


School E-Safety Policy **Redscope Primary School**

	Name of School	Redscope Primary School
	Policy review Date	November 2022
	Date of next Review	November 2023
	Who reviewed this policy?	E. E. Cobley A Bradbury

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Introduction

The main aims of our e-safety policy are:

To set out the key principles expected of all members of the school community at Redscope Primary School with respect to the use of ICT-based technologies.

To safeguard and protect the children and staff of Redscope Primary School.

To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.

To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

To 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.

To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

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

Statements

This policy applies to the whole school community including Redscope's Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.

Redscope's Senior Leadership Team and school Board of Governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safety within school will be reflected within this policy.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyberbullying, or other e-Safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate e-Safety behaviour that takes place out of school.

Review/Ownership

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

The school has appointed an e-Safety coordinator who will be responsible for document ownership, review and updates.

The e-Safety policy has been written by the school e-Safety Coordinator and is current and appropriate for its intended audience and purpose.

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.

Communication Policy

We believe that e-Safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

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

- Policy to be posted on the school website/ staffroom/ classrooms.
- 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.

Roles & Responsibilities

Senior Leadership Team

- The headteacher is ultimately responsible for e-Safety provision for all members of the school community, though the day-to-day responsibility for e-Safety will be delegated to the e-Safety coordinator.
- The headteacher and senior leadership team are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues when necessary.
- The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the e-Safety Coordinator.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious e-Safety incident.
- The headteacher and senior leadership team should receive update reports

from the incident management team

Responsibilities of the e-Safety Coordinator

- To promote an awareness and commitment to e-Safety throughout the school
- To be the first point of contact in school on all e-Safety matters
- To take day-to-day responsibility for e-Safety within school and to have a leading role in establishing and reviewing the school e-Safety policies and procedures
- To lead the school e-Safety group or committee
- To have regular contact with other e-Safety committees, e.g. the Local Authority, Local Safeguarding Children Board, Trust
- To communicate regularly with school technical staff
- To communicate regularly with the designated e-Safety governor
- To communicate regularly with the senior leadership team
- To create and maintain e-Safety policies and procedures
- To develop an understanding of current e-Safety issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in e-Safety issues
- To ensure that e-Safety education is embedded across the curriculum
- To ensure that e-Safety is promoted to parents and carers
- To monitor and report on e-Safety issues to the e-Safety group and the senior leadership team as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
- To ensure that an e-Safety incident log is kept up to date

Responsibilities of the e-Safety committee

- To ensure that the school e-Safety policy is current and pertinent
- To ensure that the school e-Safety policy is reviewed at prearranged time intervals
- To ensure that school Acceptable Use Policies are appropriate for the intended audience
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school

Responsibilities of teachers and support staff

- To read, understand and help promote the school's e-Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy

- To report any suspected misuse or problem to the e-Safety coordinator
- To develop and maintain an awareness of current e-Safety issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed e-Safety messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- 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
- To be aware of e-Safety issues related to the use of mobile phones, cameras and mobile devices
- To understand and be aware of incident-reporting mechanisms that exist within the school
- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of technical staff

- To read, understand, contribute to and help promote the school's e-Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any e-Safety related issues that come to your attention to the e-Safety coordinator.
- To develop and maintain an awareness of current e-Safety issues, legislation and guidance relevant to their work
- To maintain a professional level of conduct in your personal use of technology at all times
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system
- To liaise with the local authority or trust and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school

- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted
- To be a member of the incident-management team that meets termly to review e-Safety incidents that have occurred within school

Responsibilities of pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy
- To help and support the school in the creation of e-Safety policies and practices and to adhere to any policies and practices the school creates
- To know and understand school policies on the use of mobile phones, digital cameras and mobile devices
- To know and understand school policies regarding cyberbullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school
- To discuss e-Safety issues with family and friends in an open and honest way

Responsibilities of parents and carers

- To help and support the school in promoting e-Safety
- To read, understand and promote the school pupil Acceptable Use Policy with their children
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- To discuss e-Safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use

of technology.

- To agree to sign a home-school agreement to support the school approach to online safety and not deliberately upload or add any images, videos, sounds or texts that could upset or offend any member of the school community. To support the school's stance on the use of ICT and ICT equipment.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken are only of their child. In addition, they must follow event instructions for example, during Christmas plays no photographs to be taken during the event but an opportunity will be provided afterwards.
- If a parent adds a photograph of their child onto social media we recommend that they do not have the school emblems visible to safeguard their child.
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school.
- Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.

Responsibilities of the governing body

- To read, understand, contribute to and help promote the school's e-Safety policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the e-Safety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-Safety activities
- To ensure appropriate funding and resources are available for the school to implement its e-Safety strategy

Responsibilities of the Child Protection Officer/Safeguarding Officer

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate online contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyberbullying and the use of social media for this purpose

Responsibilities of other external groups

- The school will liaise with local organisations to establish a common approach to e-Safety and the safe use of technologies

- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate
- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds
- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school

Managing Digital Content and Communication Systems

Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done annually or as part of the home-school agreement on entry to the school.

On the school website or blog

On the school social media account e.g. Twitter

On the school's learning platform

In the school prospectus and other printed promotional material, e.g. newspapers

In display material that may be used around the school

In display material that may be used off site

Recorded or transmitted on a video or via webcam in an educational conference

- Parents and carers may withdraw permission, in writing, at any time.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites

- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- The school will store images of pupils that have left the school for 7 years following their departure for use in school activities and promotional resources.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- **D. Taylor** has the responsibility of deleting the images when they are no longer required.

Password policy

- Key Stage 1 and 2 pupils have a Class logon to all school ICT equipment. The 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.
- Do not write down system passwords. Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible. Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures, e.g. emagwriter. The school maintains a log of all accesses by users and of their activities while using the system.
- We require staff to use STRONG passwords. Passwords should contain a minimum of eight characters and be difficult to guess with numbers, letters and special characters in their passwords. The more randomly they are placed, the more secure they are. Users should create different passwords for different accounts and applications.
- Users should change their passwords whenever there is any indication of possible system or password compromise. We require staff to change their passwords twice a year.
- We require staff using critical systems to use two factor authentication.

Emerging Technologies

All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within school to ensure that any risks are managed to an acceptable level. Prior to deploying any new technologies within school, staff and pupils will have appropriate training. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be

reported to the appropriate authorities. Methods to identify, assess and minimise risks will be reviewed regularly.

Filtering Internet Access

The school uses a filtered internet service. The filtering system is provided through RGfL using Smoothwall and includes filtering appropriate to the age and maturity of the pupils. If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-Safeguarding Coordinator. All incidents will be documented in the eSafeguarding log. If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding Coordinator. The school will report such incidents to the filtering provider, RGfL. Pupils will be taught to assess content as their internet usage skills develop. Pupils will use age-appropriate tools to research internet content. The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Internet Access Authorisations

All staff and pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy regarding internet access within school. Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability. When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on prior knowledge. Key Stage 1 pupils' internet access will be directly supervised by a responsible adult. Key Stage 2 pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

E-mail

- This school provides staff with an email account for their professional use and should be aware that any use of the school email system will be monitored and checked.
- We use anonymous or group e-mail addresses, for example Teachers@redscopeprimaryschool.co.uk
- We will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- We will ensure that email accounts are maintained and up to date
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- Staff will only use official school-provided email accounts to communicate with pupils and parents and carers. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

Email usage

Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes. Pupils and staff will be reminded when using email about the need to send polite and responsible messages. Pupils must not reveal personal details of themselves or others in email communications. Communication between staff and pupils or members of the wider school community should be professional and related to school matters only. Staff email accounts should be checked regularly for new correspondence. Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments. Pupils and staff should never open attachments from an untrusted source. Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately. Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.

School website

- The headteacher and E. Cobley (website lead), supported by the Governing Body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- 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.

Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

Blogging, podcasting and other publishing of online content by pupils will take place within school and may be published on the school's website. Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff. Pupils will not use their real name when creating publicly-accessible resources. They will be encouraged to create an appropriate nickname. Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

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 /academy or local authority 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 [age appropriate] pupil Acceptable Use Agreement.
- Parents:
 - Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
 - Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Mobile Phone Usage in School

Staff Use of Personal Devices

Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices. The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones. Personal mobile phones will only be used during lessons with prior permission from the headteacher in exceptional circumstances. No images or videos should be taken on mobile phones or personally-owned mobile devices.

Pupils' Use of Personal Devices

Pupils are advised not to bring his or her mobile phone or personally-owned device into school. Any device brought into school needs to be stored securely by the class teacher. The school accepts no responsibility for the loss, theft or damage of pupils' mobile phones or mobile devices. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries

and consequences. If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will then be released to parents or carers. If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Use of Laptops/iPads

The use of laptops and iPads by all staff is restricted by an acceptable use agreement which is signed by relevant staff. Laptops and iPads left in school overnight must be locked away. iPads must not be connected to individual iTunes accounts and requests for apps must be in writing to the ICT coordinator. If staff are unable to attend work for an extended period (over 2 weeks) laptops and iPads should be returned to school.

Teaching & Learning

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a series of specific eSafeguarding-related lessons in every year group as part of the ICT curriculum / PSHE curriculum / other lessons ensuring the following objectives are met:
 - EYFS
 - Uses ICT hardware to interact with age-appropriate computer software.
 - KS1
 - Use technology safely and respectfully, keeping personal information private; identify where to go for
 - help and support when they have concerns about content or contact on the internet or other online technologies.
 - KS2
 - Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
 - Use technology safely, respectfully and responsibly; recognize acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.
- We promote Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions

may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.

- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which will be shared with every pupil and a collective user policy will be displayed when a pupil logs on to the school network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Staff Training

- Our staff receive regular information and training on e-Safety issues in the form of annual updates/ termly staff meetings, CPD and emails from the e-Safety coordinator, as appropriate.
- As part of the induction process all new staff receive information and guidance on the e-Safety policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the

safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

Incidents

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- E-Safety Coordinator and headteacher act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to the headteacher and e-Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the headteacher, unless the concern is about the headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used found on the below link:

<https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis>

This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
- 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?
- 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 or 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 come to light).

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.

Data Protection and Information Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school has deployed appropriate technical controls to minimise the risk of data loss or breaches. Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information. All access to information systems should be controlled via a suitably complex password. Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school. All physical information will be stored in controlled access areas. All communications involving personal or sensitive information (email, fax or post) should be appropriately secured. All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted laptops or encrypted hard-drives. Devices taken off site, e.g. laptops, tablets, etc, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Management of Assets

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. All redundant ICT equipment will be disposed of through an authorised agency and ICT equipment that may have held personal data will have the storage media irretrievably destroyed. Disposal of any ICT 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.