Online - Safety Policy

(This policy applies to all pupils including those in the EYFS)

Adopted	September 2014
Revised	November 2016
Reviewed	October 2017
Next Review	October 2018
Owner	Deputy Head Pastoral

Contents

1. Introduction and Overview

The purpose of this policy is to:

- Outline the guiding principles for all members of the school community regarding the use of ICT.
- Safeguard and protect the students and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of the policy

This policy applies to all members of school community - staff, students, volunteers, parents and carers, visitors, community users - who have access to and are users of school's ICT systems.

For clarity, the online-safety policy uses the following terms unless otherwise stated:

- **Users** - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors..

- **Parents** – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

- **School** – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

- **Wider school community** – pupils, all staff, governing body, parents.

At Mount Kelly we use technology and the Internet extensively across all areas of the curriculum. online safeguarding, known as online-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.

- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

2. Review and Monitoring, Roles and responsibilities

Safeguarding Sub-Committee of the Governing Body

The **Safeguarding Sub-Committee of the Governing Body** is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any online-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online-safety incidents are appropriately dealt with and ensure the policy is effective in managing those incidents.

Deputy Head Pastoral (DHP)

- Reporting to the governing body, the DHP has overall responsibility for online-safety within the School. The work of the DHP will be supported by the Heads of ICT at the College and the Prep in their capacity as Online-Safety Officers.

The DHP will ensure that:

- Online-safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- The Online-safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All online-safety incidents are dealt with promptly and appropriately.

Online-safety Officer

The online-safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize himself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the SLT.
- Advise the SLT and Safeguarding Committee on online-safety matters.
- Engage with parents and the school community on online-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Ensure any technical online-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the ICT Technical Support.
- Make himself aware of any reporting function with technical online-safety measures, i.e. internet filtering reporting function; liaise with the Head Master and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any online-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online-safety officer and Head Master.
    - Passwords are applied correctly to all users regardless of age

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the DHP.
- Any online-safety incident is reported to the DHP (and an online-safety Incident report is made), or in his/her absence to the Principal Deputy Head. See page 14.
- The reporting flowcharts contained within this online-safety policy are fully understood.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

online-safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will support parents in understanding and acquiring the skills and knowledge they need to ensure the safety of children outside the school environment. Through access to courses and a dedicated section to Online Safety on the School website the school will keep parents up to date with new and emerging online-safety risks, and will involve parents in strategies to ensure that pupils are empowered to protect themselves. The link below will take Parents directly to the guidance provided by the School.

http://www.mountkelly.com/Parents-Internet-Safety

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will support the School in its application of the Acceptable Use Policy.

The Safeguarding Committee

Chaired by the Governor responsible for safeguarding, online-safety will fall within the remit of this sub-committee of the Governing Body, which will:

- Advise on changes to the online-safety policy.
- Establish the effectiveness (or not) of online-safety training and awareness in the school.
- Recommend further initiatives for online-safety training and awareness at the school.

Technology

Mount Kelly uses a range of devices. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

- **Internet Filtering** – we use Smoothwall software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The online-safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

- **Email Filtering** – software prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

- **Encryption** – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

- **Passwords** – all staff and pupils will be unable to access the School's internet without a unique username and password. Staff and student passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The online-safety Officer and IT Support will be responsible for ensuring that passwords are changed.

- **Anti-Virus** – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any

concerns. All USB peripherals such as keydrives (if you allow them) are to be scanned for viruses before use.

3. Education and Curriculum

Student online safety curriculum

The school has a clear, progressive online safety education programme primarily as part of the PSHE curriculum but referenced in all areas of school life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

The school will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities using the Acceptable Use Agreement.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.

4. Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to members of the School community after agreeing to the Acceptable user Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Pupils are permitted to use the school email system, and as such will be given their own email address and they must confirm to accepted e-mail protocols.

Photos and videos – Digital media such as photos and videos are covered in the schools' *Use of Pupils' Images Policy*. Every new parent is asked to sign a copy of the School's Terms and Conditions, in which they agree that the School may make use of images for their children in publications and on the School's website.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out Internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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

Staff are allowed to take digital and video images to support educational and marketing aims, but must follow school policies concerning the taking, sharing, distribution and publication of those images. All staff are given guidance on the school's policy on taking, using and storing images of children. This includes:

- Staff should, whenever possible, use school cameras/recording devices rather than personal equipment*.
- Digital images of children must be stored on the password protected area of the school's network.
- Digital images of children should not be stored on personal/home computers/hard drives, except where these images have been publicly available to parents or others on the school's website or in the weekly newsletter. It is acceptable to have play or team photographs for instance.
- Hard copies of children's images should be stored in a locked filing cabinet on the school premises, except where these are used for publicity purposes around the School: e.g. team and play photographs.

***Staff working with children in the EYFS must not use personal recording equipment at any time.**

- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully – and the general parental consent form must have been completed.
- Pupils' full names should not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents will be obtained before photographs of pupils are taken or published, for example on the school website.

Social Networking – there are many social networking services available; Mount Kelly is fully supportive of social networking as a tool to engage and collaborate with learners, and to

engage with parents and the wider school community. The following social media services are permitted for use within Mount Kelly and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the online-safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and pupils in school.
- Twitter – used by the school as a broadcast service (see below).
- Facebook – used by the school as a broadcast service (see below).

In addition, the following is to be strictly adhered to:

- Permissions (via the school photographic policy) must be consulted before any image or video of any child is uploaded. This may be found on the School's *Use of Pupils' Images policy*, which is on the School website.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any online-safety incident is to be brought to the immediate attention of the Deputy Head Pastoral, or in his/her absence the Principal Deputy Head.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Mount Kelly will have a programme of training which is suitable to the audience.

online-safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The online-safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head Master and chairman of the Safeguarding Committee for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

5. Acceptable use policy and Agreement

This policy outlines what are acceptable and unacceptable uses of ICT facilities within Mount Kelly. It is relevant to pupils, staff, governors and visitors. Whilst we aim to support the full use of the vast educational potential of new technologies we also have a responsibility to provide safeguards against risk, unacceptable material and activities. These guidelines are designed to protect pupils, staff and visitors from onlinonline-safety incidents and promote a safe online-learning environment for pupils.

At Mount Kelly we believe that pupils should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make productive decisions in the ways they decide to use digital technologies; we should all be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our school.

Examples of acceptable use are:

- Using web browsers to obtain information from the Internet
- Accessing databases for information as needed.
- Using e-mail for contacts.
- Using the school's network to promote the exchange of information to further education and research and is consistent with the mission of the school.
- Using the school's network to access outside resources that conform to this "Acceptable Use Policy".
- Using the network and Internet in a manner, which respects the rights and property of others.
- Keeping all accounts and passwords confidential and inaccessible to others.
- Showing responsibility by making backup copies of material critical to you.
- Showing responsibility by taking precautions to prevent viruses on the school's equipment.
- Upon receipt of an attachment checking to making sure it is from a known source.
- Backing out of an accidentally encountered site that contains materials that violate the rules of acceptable use, and notifying a teacher or supervising adult of the occurrence immediately.
- Logging out or locking computers when they are left unattended
- Recognise that electronic communications sent through or stored on the school's network will be treated as school related and may be monitored or examined by the Head Master or his authorised delegates for operational, maintenance, compliance, auditing, security and/or investigative purposes
- Reporting any damage to or loss of computer hardware immediately
- Saving documents onto appropriate storage areas of the school network or other appropriate storage systems
- Reporting any inappropriate behaviour and online bullying to the Deputy Head Pastoral
- Take reasonable care that there is no damage or loss of any equipment on loan from school

Examples of unacceptable use are:

- Use of the Internet for purposes that are illegal, unethical, harmful to the school, or nonproductive.
- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Recording, filming or take photographs on school premises without permission and with consent of the parent or carer.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list without permission from the Principal Deputy Head.
- Relocating school information and communication equipment without prior permission
- Conducting a personal business using school resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Using inappropriate language: do not swear, use vulgarities or sexual innuendos.
- The sending of material likely to be offensive or objectionable to recipients.
- Using programs that harass school users or infiltrate a computing system and/or damage the software components is prohibited.
- Changing original software setting/configuration of school owned computers
- Doing harm to other people or their work.
- Do not install software on school computers unless authorised by the ICT Team.
- Doing damage to the computer or the network in any way.
- Interfering with the operation of the network by installing illegal software, shareware, or freeware.
- Plagiarisation and violation of copyright laws.
- Conversation in email using all upper case letters. This is considered shouting.
- Sharing your passwords with another person. Doing so could compromise the security of your files.
- Wasting limited resources such as disk space or printing capacity.
- Trespassing in another's folders, work, or files.
- Removing software CDs from their rightful location
- Giving out personal information such as your home address or telephone number. Use the school's address instead, but not the school's phone number.
- Downloading material from the Internet without specific authorisation from the ICT manager.
- Viewing, sending, or displaying offensive messages or pictures.
- Accessing sites that contain pornography; that spread hatred; that promote discrimination; that give instruction for acts of terrorism, harassment, murder, suicide, or other illegal activity.

6. **Youth produced sexual imagery (sexting)**

The practice of children sharing images and videos via text message, email, social media or mobile messaging apps has become commonplace. However, this online technology has also given children the opportunity to produce and distribute sexual imagery in the form of photos and videos. Such imagery involving anyone under the age of 18 is illegal.

Youth produced sexual imagery refers to both images and videos where;

- A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18.
- A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult.
- A person under the age if 18 is in possession of sexual imagery created by another person under the age of 18.

All incidents of this nature should be treated as a safeguarding concern and in line with the UKCCIS guidance 'Sexting in schools and colleges: responding to incidents and safeguarding young people'[1].

Cases where sexual imagery of people under 18 has been shared by adults and where sexual imagery of a person of any age has been shared by an adult to a child is child sexual abuse and should be responded to accordingly.

If a member of staff becomes aware of an incident involving youth produced sexual imagery they should follow the child protection procedures and refer to the DSL as soon as possible. The member of staff should confiscate the device involved and set it to flight mode or, if this is not possible, turn it off. Staff should not view, copy or print the youth produced sexual imagery.

The DSL should hold an initial review meeting with appropriate school staff and subsequent interviews with the children involved (if appropriate). Parents should be informed at an early stage and involved in the process unless there is reason to believe that involving parents would put the child at risk of harm. At any point in the process if there is concern a young person has been harmed or is at risk of harm a referral should be made to MASH or the Police as appropriate.

Immediate referral at the initial review stage should be made to MASH/Police if;

- The incident involves an adult;
- There is good 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 education needs);
- What you know about the imagery suggests the content depicts sexual acts which are unusual for the child's development stage or are violent;
- The imagery involves sexual acts;
- The imagery involves anyone aged 12 or under;
- There is reason to believe a child is at immediate risk of harm owing to the sharing of the imagery, for example the child is presenting as suicidal or self-harming.

If none of the above apply then the DSL will use their professional judgement to assess the risk to pupils involved and may decide, with input from the Head Master, to respond to the incident without escalation to MASH or the police.

[1]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545997/Sexting_in_schools_and_colleges_UKCCIS__4_.pdf

In applying judgement the DSL will consider if;

- there is a significant age difference between the sender/receiver;
- there is any coercion or encouragement beyond the sender/receiver;
- the imagery was shared and received with the knowledge of the child in the imagery;
- the child is more vulnerable than usual i.e. at risk;
- there is a significant impact on the children involved;
- the image is of a severe or extreme nature;
- the child involved understands consent;
- the situation is isolated or if the image been more widely distributed;
- there other circumstances relating to either the sender or recipient that may add cause for concern i.e. difficult home circumstances;
- the children have been involved in incidents relating to youth produced imagery before.

If any of these circumstances are present the situation will be escalated according to our child protection procedures, including reporting to the police or MASH. Otherwise, the situation will be managed within the school.

The DSL will record all incidents of youth produced sexual imagery, including both the actions taken, actions not taken, reasons for doing so and the resolution in line with safeguarding recording procedures.

7. ADVICE TO STAFF

Searching a device

- In a school-based context, it is highly likely that the image will have been created and potentially shared through mobile devices. It may be that the image is not on one single device: it may be on a website or on a multitude of devices; it may be on either a school-owned or personal device.
- If any illegal images of a child are found the police will be informed immediately.

Never…

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest that there is an immediate problem.
- Print out any material for evidence.
- Move any material from one storage device to another.

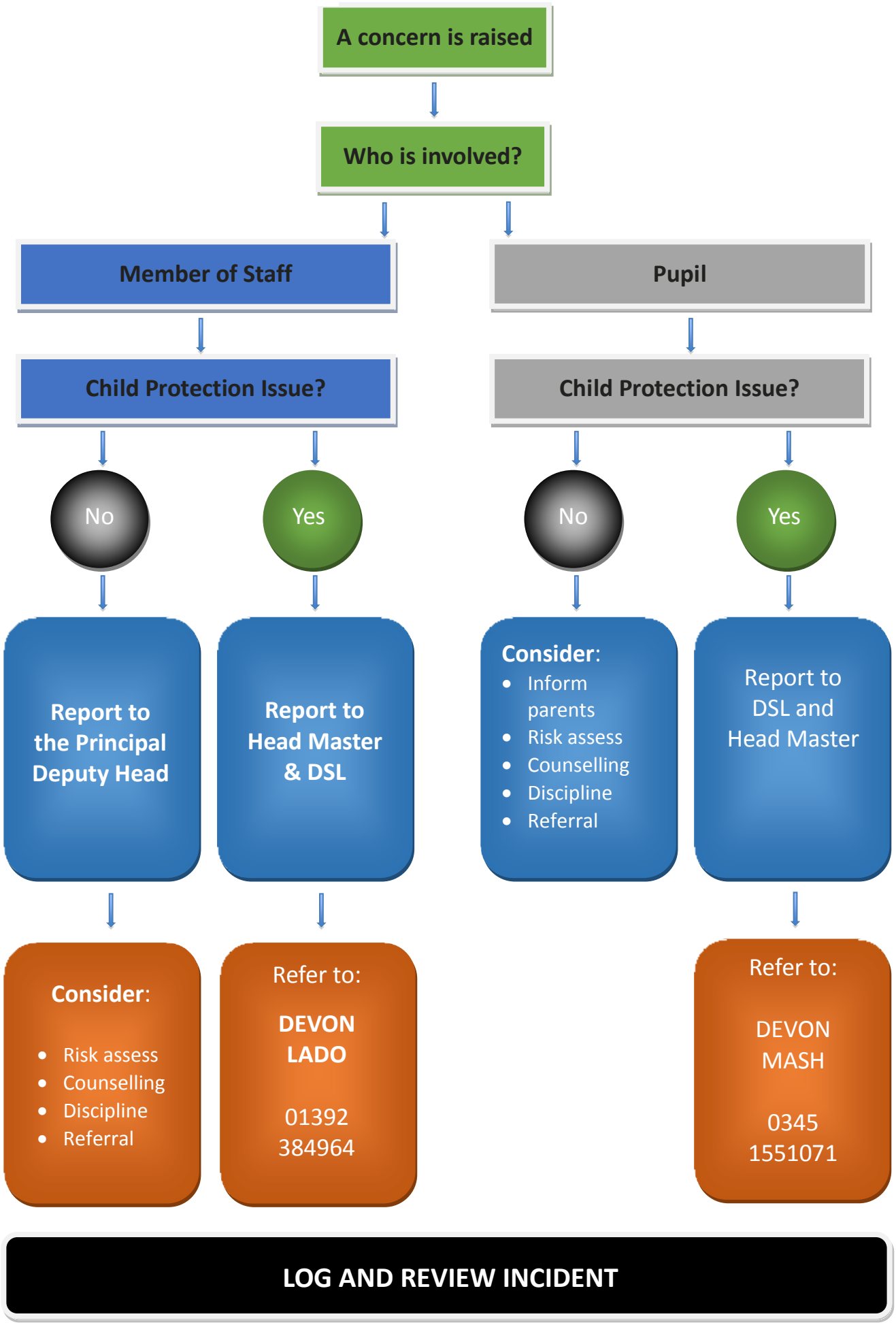
Always...

- Confiscate and secure the device(s)
- Inform the DSL.
- Record the incident
- Act in accordance with school safeguarding and child protection policies and procedures

Containing the incident and managing student reaction

Sadly, there are cases in which victims of youth produce sexual imagery have had to leave or change schools because of the impact the incident has had on them. The pupil will be anxious about who has seen the image and where it has ended up. They will seek reassurance regarding its removal from the platform on which it was shared. They are likely to need support from the school, their parents and their friends. Creating a supportive environment for students in relation to the incident is very important and staff should be vigilant and report any further concerns after an incident has occurred.

8. Online Incident Pathway



9. Online-Safety Incident Log

Reported By: *(name of staff member)*	**Reported To:** *(DHP, PDH, HM)*
Date & Time:	**Location:**
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)	
Action Points	
Outcome:	

Signature **Staff reporting**		**Date:**	
Signature **DHP**		**Date:**	