Radlett Lodge School

Online Safety Policy

The Designated Child Protection Officer for the school are Ellie Freeman, Laura Smart, Leigh-Anne Lamb, Kylee Lyon, Stuart Mainwaring and Jeremy Keeble

This policy was agreed in September 2017

This policy is due for review in September 2018

Overview
Students at the school have the right to access new and emerging technologies as part of their education and care. These technologies are a vital part of the lives of many people with autism and the school is committed to promoting students development of the skills, knowledge and understanding to communicate, create, investigate, play and relax online. The school provides technology for students as well as providing a network that allows them to use their own devices.

The school recognises that online activity brings with it potential risks, which fall into three main categories:

Content: being exposed to illegal, inappropriate or harmful material
Contact: being subjected to harmful online interaction with others
Conduct: behaving online in a way that that increases the likelihood of, or causes, harm.

Our primary aim with regard to online safety is to give students the ability to stay safe online – both inside the school and beyond. We aim to do this through education, embedding online safety in every aspect of the curriculum and working with parents/carers, siblings and others to promote safe use of technology. This online safety policy (and the associated procedures) lay out the ways in which we keep students safe while providing this education.

As a school we have specific, statutory responsibilities to ensure and promote the safety and well-being of our pupils and this applies to the online environment. A number of laws and statutory government guidance applies in this area, see appendix 2 for a full list of legislation and guidance.

Aims
The school aims to provide students with the skills, knowledge and understanding to keep themselves safe online within the school and beyond, now and in the future. This policy gives guidance on providing a safe environment in which students may develop their own online safety skills.

Roles & Responsibilities

Executive Director – Education, NAS SMG, NAS ICT Advisor
Executive Director – Education and the NAS SMG are responsible for the approval of the online safety Policy, for reviewing the effectiveness of the policy and for overseeing revisions of the policy. They will also act as a 'friendly critic' (in the role an online safety governor would play) and ensure:

- regular meetings with the school Online Safety Coordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering and change logs
- taking part in reviews of the online safety policy and procedures

Principal and SLT

The Principal is responsible for ensuring the safety (including online safety) of members of the school community. Day to day responsibility for online safety will be delegated to the Online Safety Coordinator.

The Principal and Senior Leaders within the school are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Principal and Senior Leaders will ensure that there are systems in place to allow for monitoring and support of those staff who carry out the internal online safety role.

The Senior Leaders will receive regular monitoring reports from the Online Safety Coordinator and act on them accordingly.

The Principal and Senior Leaders will be aware of the procedures to be followed in the event of a serious online safety incident occurring.

The Principal and Senior Leaders oversee the safe use of electronic and social media by staff and take action immediately if they are concerned about bullying or risky behaviours

Online Safety Coordinator
The school will have a named member of staff with day to day responsibility for online safety. This role may be combined with the Designated Safeguarding Lead role. This is primarily a safeguarding role, not a technical role, although the coordinator should have a good understanding of technical issues.

The Online Safety Coordinator:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority as appropriate
- liaises with IT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with the Executive Director – Education, NAS SMG and/or NAS ICT Advisor to discuss current issues, review incident logs and filtering
- attends relevant meetings
- reports regularly to the Senior Leadership Team

Staff

All teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and procedures
- they report any suspected misuse or problem to the Online Safety Coordinator for investigation
- digital communications with students (for example by email or social networking) should be on a professional level
- online safety issues are embedded in all aspects of the curriculum and other school activities
- they help students understand and follow the school online safety and acceptable use policy
- they strive to ensure students have an understanding of behaving legally and responsibly online
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, tablets, games machines, cameras and other devices and that they monitor their use and implement current school policies with regard to these devices
- they ensure that their own behaviour online is in accordance with professional standards, both within and beyond the school.

Students

The school will attempt to give students the knowledge, skills and understanding to keep themselves safe online, both in the school and outside it.

Students are responsible for using ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems. For some students it may be expected that parents/carers would sign on behalf of the student.

Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to go about doing so. As far as possible students will be expected to know and understand school policies on the use of mobile phones, tablets, games machines, cameras and other devices.

Students should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet in an appropriate way. The school are aware that parents and carers may not fully understand technical issues and be less experienced users of ICT than their children. Parents/carers often either

underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what to do about it. The school will therefore take every opportunity to help parents understand these issues through collaborative working and training, which may include siblings or other family members as appropriate.

Parents/carers are responsible for:

- working with the school to ensure that their children have the best opportunity to learn to keep themselves safe online
- signing the Student Acceptable Use Policy (if necessary)
- accessing the school's online resources in accordance with the relevant school policies
- reviewing and revising the Online Safety Policy. All revisions will take full account of their views of parents/carers and students and incorporate them into revised polices

Criteria for Success

1. There is clear evidence that staff understand and act on the online safety policy. This may come from formal assessment of staff after training, review of incident logs and 'white hat' security testing. It is the responsibility of the Online Safety Coordinator to collect this evidence and of the Executive Director – Education, NAS SMG, NAS ICT Advisor to evaluate it.

2. Students are able to demonstrate increased understanding of online safety issues through formal and informal assessments.

3. Information on incidents show that they are being reported appropriately and that incidents are followed up.

4. This policy is reviewed and revised according to the set timescales.

5. The school uses tools such as the SWGfL 360 Degree Safe self-assessment to review online safety provision and identify possible improvements.

Procedures

In line with previously published best practice (e.g.: Becta's E-safety - Developing whole-school policies to support effective practice, available at: http://webarchive.nationalarchives.gov.uk/20101102103654/http://publications.becta.org.uk/download.cfm?resID=25934) there are three key aspects to online safety:

1. Education
2. Technical tools (e.g.: filtering, logging)
3. Review and revision of policy and procedure

While all three are intertwined in good practice, the school places great emphasis on the educational aspects, in particular because the technical tools may not always be present when a student is online (for example at home or in the community). The ability to stay safe online is something that students must be allowed to develop. This initially involves some degree of risk, however in the long term not giving students the skills to be safe online is likely to present an even greater risk. An analogy may be made with teaching independent travel and road safety: while there are very real, immediate and deadly risks involved in this, we still see the benefit of being safe on the road as being worth the risk in teaching those skills.

All students will therefore receive appropriate online safety education while at the school and this will be embedded into all aspects of the curriculum. Details of this can be found in the relevant curriculum documents.

The key skills that will be developed are:

- The importance of using technology safely and respectfully
- Understanding implications of sharing personal information
- Knowing where to go for help if they have concerns about content or contact on the internet
- Understanding the law as it applies online, in particular copyright and intellectual property rights.
- An awareness of the dangers and consequences of plagiarism, copyright infringement, piracy, and the reliability and bias of information sources.
- Understanding how to become a safe and responsible online citizen.
- How to develop positive, healthy and age appropriate online relationships

Responsibility for online safety is the responsibility of all members of the school. This means that education about online safety is the responsibility of all members of the school. The school actively encourages students to act as mentors to other students in many aspects of their education and in particular with regard to behaviour online. Mentors, cyber-buddies, e-pals and other input may come from students at the school or from vetted individuals from outside.

On admission at the school all students will have a customised Acceptable Use Policy (AUP) to sign which is provided by each school. The purpose of this is to explicitly state what behaviour is allowed, expected and supported. It should form the basis of discussion around online behaviour and the use of technology within the school and beyond. A template is available from the ICT Advisor and should be modified for each student so that it is meaningful to the student. Sections may be added to deal with specific behaviours for individual students as appropriate.

Dealing with online incidents
All staff must be aware of students' use of online technologies. There are two essential things to look out for:

1. Students are encouraged to report anything that happens to them online that upsets them. This could range from something that is illegal (for example an attempt at sexual grooming, sexting, images of child abuse, financial embezzlement) through inappropriate behaviour (for example abusive behaviour online, bullying) to innocuous incidents that some people with autism may find distressing (for example being upset at a news story, seeing an image of a disliked food). It is crucial that all staff should be receptive to students and approachable to ensure students report when necessary. Staff should also be aware of the correct procedure to deal with students reporting incidents.

2. Students may not report an online activity that upsets them or which they know is wrong. This may be because they are not immediately aware of becoming upset or distressed, although their behaviour may indicate this. It may be that they perceive the 'upset' as 'normal'. It may be because they do not want to report it for any reason. Staff must be aware of behavioural, social or emotional indicators that a student has encountered something online that should be investigated. When in doubt, any incident that causes concern should be reported to a line manager or the Online Safety Coordinator.

Bear in mind also that safeguarding issues and abuse/neglect are rarely standalone events.

The following pages set out the procedures for reporting incidents in simple flow chart fashion:

Chart 1. Illegal activity online procedure
Chart 2. Inappropriate activity online procedure
Chart 3. Student as victim procedure

1. Illegal activity online procedure

When an incident is reported staff (ideally the online safety coordinator and/or the Principal) will need to decide if the incident involved any **illegal** activity.

In this context **illegal** activity includes:

- Downloading child sexual abuse images
- Passing onto others images or video containing child sexual abuse images
- Inciting racial or religious hatred
- Extreme cases of cyber bullying
- Promoting illegal acts including terrorism

If you are not sure if the incident has any illegal aspects – immediately report it anyway to the online safety coordinator, the Principal or the Child Protection Officer.

Was **illegal** material or activity found or suspected?

Yes

No

Inform police (**999)** and **Principal**/senior on site.

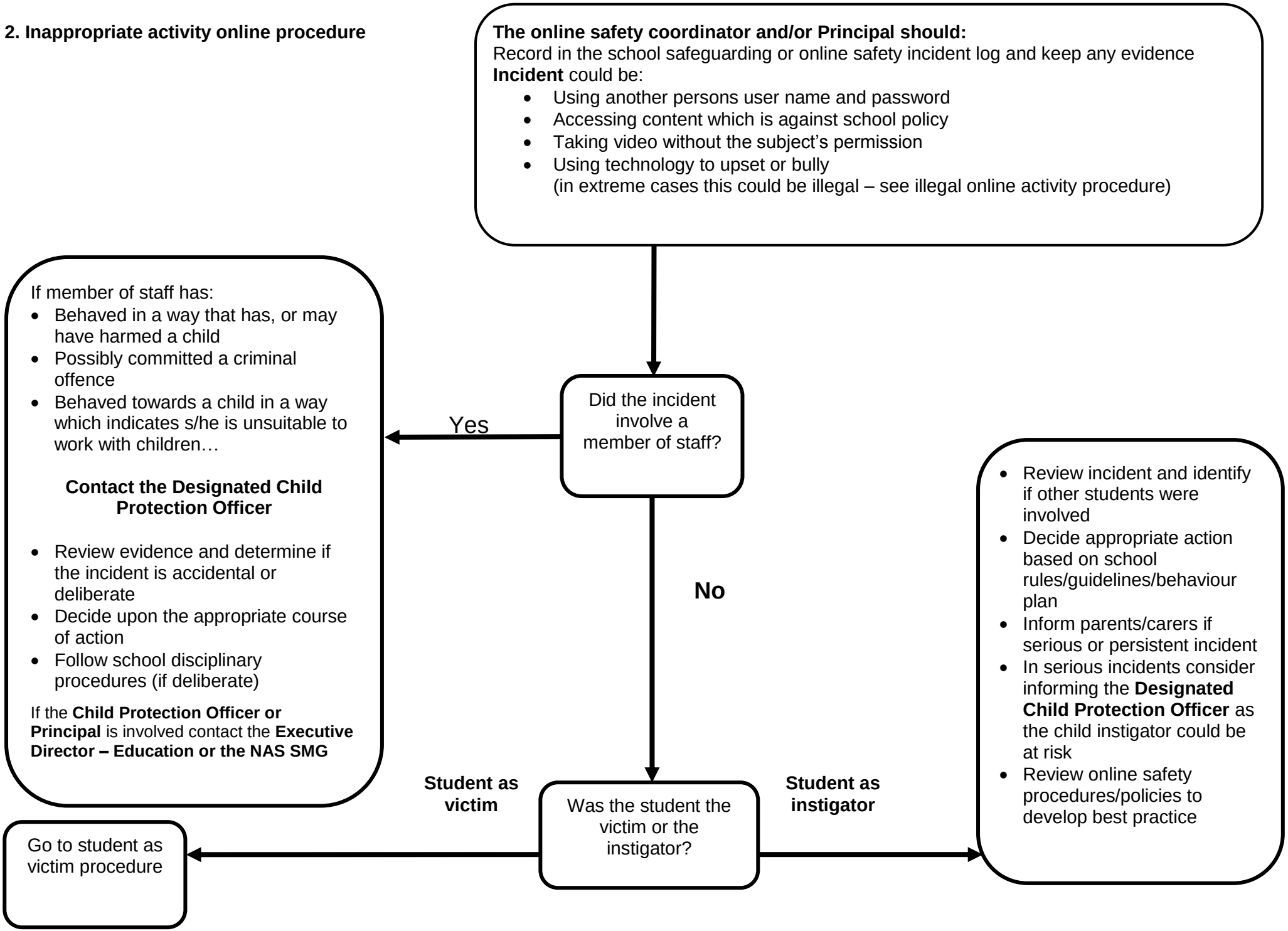
Follow the advice given by the police otherwise:

- Confiscate any computer or other device
- Power the device off at once. Do not shut it down as normal as this may remove evidence
- Lock the device away securely labelling it not to be touched
- If related to school network disable the user(s) account
- Save **any** evidence but **DO NOT** view or copy. Let the police review the evidence.

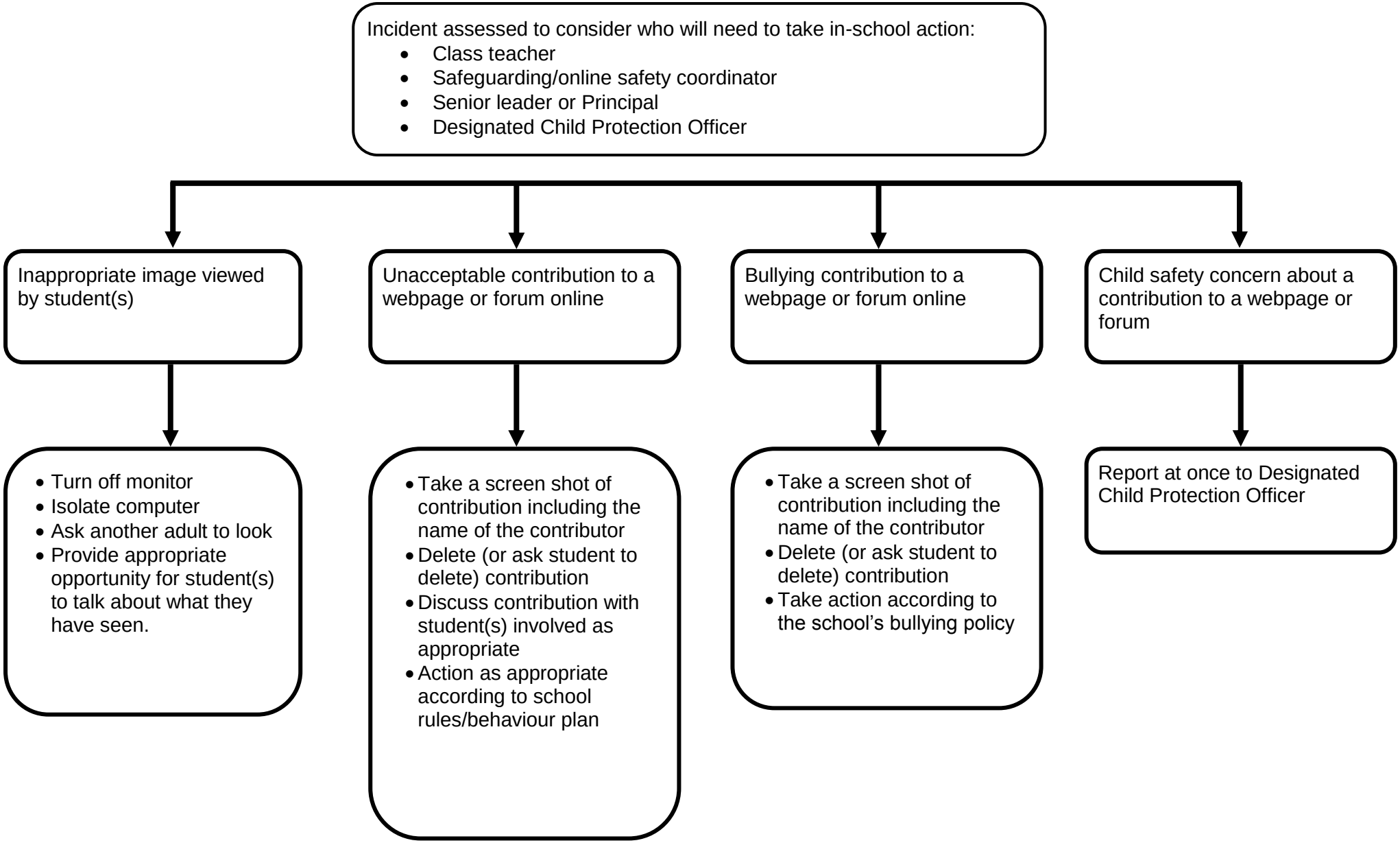
If a student is involved inform the **MASH on 01438 737511**

Follow the flowchart relating to **inappropriate incidents.**

2. Inappropriate activity online procedure



3. Student as victim procedure



Technical tools
The school has a filtering policy that allows different levels of access to different groups of users. Users are given more (or less) access depending on their ability to stay safe online. In this way the filtering of content is linked directly to students' learning. For example students may be given access to social networking sites as they have demonstrated that they are able to behave safely and responsibly on such sites. Students may be given differential access according to their level of online safety knowledge.

Changes to filtering for these groups must be logged in the filtering log, as must changes to a student's level of access along with the reason for the change in access. The Online Safety Coordinator is responsible for these logs being kept accurate and up-to-date, although they do not have to be the person actually logging the information. Senior leaders and the Executive Director – Education, NAS SMG, NAS ICT Advisor will check these logs on a regular (at least 3 times a year) basis.

Logs of online activity are available on request from the ICT technician or the ICT providers. These may be used to monitor and assess a student's online behaviour or to provide evidence in the case of an incident. Request for logs must be made through the Principal or the Online Safety Coordinator.

Review and revision of policy and procedure
The Online Safety Coordinator has the leading role in reviewing the school online safety policies and documents. This process is overseen by the Principals and the Executive Director – Education, NAS SMG, NAS ICT Advisor.

Review will occur at least once a year and after a serious incident is recorded.

Review should take account of the following:

1. The effectiveness of the current policy and procedure
2. Changes to legislation
3. Advice on best practice from other agencies (e.g.: OfSTED) or tools such as SWGfL's 360 Degree Safe
4. The views of the whole school community. This includes students and parents/carers as well as other family members as appropriate.

All members of the school community, including parents/carers and students will be involved in the review and revision of this policy.

Appendix 1: Adherence to the 'Keeping Children Safe in Education' / UK Safer Internet Centre criteria

Illegal content

IWF list and "police assessed list of unlawful terrorist content": blocked at source by the NAS Netsweeper product.

Inappropriate Online Content

Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.

Covered by the Netsweeper category: Hate Speech

Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances

Covered by the Netsweeper category: Substance Abuse

Extremism: promotes terrorism and terrorist ideologies, violence or intolerance

Covered by the Netsweeper categories: Extreme, Hate Speech, Criminal Skills

•Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content

Covered by the Netsweeper categories: Criminal Skills, Peer to Peer, Infected Hosts. Malware is blocked at source by the NAS systems.

Pornography: displays sexual acts or explicit images

Covered by the Netsweeper category: Pornography

Piracy and copyright theft: includes illegal provision of copyrighted material

Covered by the Netsweeper categories: Criminal Skills, Peer to Peer, Infected Hosts

Self Harm: promotes or displays deliberate self-harm (including suicide and eating disorders)

Covered by the Netsweeper category: Extreme (specifically this will block self-harm sites, anorexia, bulimia and other content that can prove harmful to children).

•Violence: Displays or promotes the use of physical force intended to hurt or kill

Covered by the Netsweeper category: Extreme

Filtering System Features

Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role

The school can provide this through student logins or by access to different SSIDs with different levels of filtering on each.

Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content

Control is delegated to the school. Staff can change filters themselves. Different sites can have different filtering policies to permit or deny access to specific content.

Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking

Netsweeper publishes classification of filtering and categorises on the Netsweeper website as well as a view in real time of new content categorised. This can be found at: http://www.netsweeper.com

Identification - the filtering system should have the ability to identify users

All users who login and all devices on BYO can be identified.

Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies

The Local Area Network includes application visibility and control which allows the blocking of mobile and app technologies.

Multiple language support – the ability for the system to manage relevant languages

The system supports the following languages: Arabic, English, French, German, Japanese, Persian, Polish, Russian, Simplified Chinese, Spanish, Turkish and Vietnamese. The system will shortly also support Somali, Bangla, Croatian, Estonian, Swedish, Irish, Norwegian, Thai, Bulgarian and Traditional Chinese

Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices

All filtering is done at the network level (LAN and WAN). There is no software on users' devices.

Reporting mechanism – the ability to report inappropriate content for access or blocking

Any member of staff can ask the local school technician or the central IT Department to block content.

•Reports – the system offers clear historical information on the websites visited by your users

Demand and scheduled reports are available, in graphical or text format across a wide range of predefined or custom designs.

Appendix 2: Legislation

The following appendix lays out some of the legislative framework under which this Online Safety Policy has been produced.

Note that, in most cases, an action that is illegal if committed offline is also illegal if committed online. For this reason not all laws are covered here, only those that specifically relate to online behaviour.

Computer Misuse Act 1990
This Act makes it an offence to:
Erase or amend data or programs without authority;
Obtain unauthorised access to a computer;
"Eavesdrop" on a computer;
Make unauthorised use of computer time or facilities;
Maliciously corrupt or erase data or programs;
Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:
Fairly and lawfully processed.
Processed for limited purposes.
Adequate, relevant and not excessive.
Accurate.
Not kept longer than necessary.
Processed in accordance with the data subject's rights.
Secure.
Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
Establish the facts;
Ascertain compliance with regulatory or self-regulatory practices or procedures;
Demonstrate standards, which are or ought to be achieved by persons using the system;
Investigate or detect unauthorised use of the communications system;
Prevent or detect crime or in the interests of national security;
Ensure the effective operation of the system.
Monitoring but not recording is also permissible in order to:
Ascertain whether the communication is business or personal;
Protect or support help line staff.
The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:
Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice including by phone or using the Internet. It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, that they are in a position of trust with. (Typically, teachers, social workers, health professionals, fall in this category of trust). Any sexual intercourse with a child under the age of 13 is an offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:
The right to a fair trial
The right to respect for private and family life, home and correspondence
Freedom of thought, conscience and religion
Freedom of expression
Freedom of assembly
Prohibition of discrimination
The right to education
These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

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

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent / carer to use Biometric systems

Guidance

Ofsted (August 2015) Inspecting safeguarding in early years, education and skills settings
Embeds online safety in the inspection process for schools