Online Safety Procedure
Helen Allison School

Approved by:	Principal	**Date:** 04.10.18
Last reviewed on:	04.10.18	
Next review due by:	04.10.19	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, parents, visitors and our school governor
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Principal

The Principal is responsible for ensuring that staff understand this procedure and that it is being implemented consistently throughout the school.

3.2 The Designated Safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding procedure.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this procedure and that it is being implemented consistently throughout the school
- Working with the Principal, IT support and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this procedure
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour procedure
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal

This list is not intended to be exhaustive.

3.4 The NAS IT support

NAS IT support is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on at least a monthly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this procedure
- Implementing this procedure consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this procedure
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour procedure

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this procedure
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this procedure, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- 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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This procedure will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this procedure can be raised with any member of staff or the Principal.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Safeguarding procedure)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Safeguarding procedure. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so. (Appendix 5)

6.3 Examining electronic devices

The Principal, DSL and members of SLT have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff with authority must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

If your child brings in a device then this will need to be locked away on arrival and will be returned to them when they leave at the end of the day.

We cannot permit students to have devices that they are able to access social media sites during school hours e.g. Facebook, Snap Chat etc. also if the device allows them to take photos or videos of other students or staff members this is against GDPR.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger an action, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from IT Support.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse **(appendix 3 & 4)**

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in this document. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

The school governor will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding procedure.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the ICT Manager. At every review, the policy will be shared with the school Governor.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding procedure
- Positive Behaviour procedure
- Staff disciplinary procedure
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable Use Agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet:

Agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purposes
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school this will be handed in to staff on arrival unless an agreement has been made between the parents/carer and the school:

- I will not use any personal device without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I understand that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to certain actions which may include loss of access to the school network, access to the internet and contact will be made with parents/carers and in the event of illegal activities involvement of the police or other parties.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I will work with the school to support my child's use of social media outside school hours

The school has various methods for communication. These systems foster mutual respect and ensure the best learning experiences for the child.

We kindly request that parents do not post pictures, make comment on or name pupils, other than their own children, on social networking sites, including closed groups, where these photographs have been taken at a school event.

There are school policies and procedures that inform parents and carers regarding appropriate

channels of communication to resolve complaints. We kindly request that parents and carers share complaints through official school channels rather than posting them on social networking sites. Parents should not post malicious or fictitious comments on social networking sites, including closed groups, about any member of the school community. The school reserve the right to seek legal recourse should the school be named in a defamatory manner.

Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: Agreement for staff, school governor, volunteers and visitors
Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I understand that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy.

I will let the Designated Safeguarding Lead (DSL) and IT support know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will not use personal devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home

I will only use school approved equipment for any storage, editing or transfer of digital images/videos/documentation and ensure I only save photographs and videos of children and staff on the school equipment.

I understand that I have a responsibility for my own and others' safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and that I read and understand the school's most recent online safety and other related policies and procedures as well as relevant training.

I understand that failure to comply with this agreement could lead to disciplinary action.

The school has various methods for communication. These systems foster mutual respect and ensuring the best learning experiences for the child.

We kindly request that staff, volunteers or governors do not post pictures or name pupils, other than their own children, on social networking sites, including closed groups, where these photographs have been taken at a school event.

There are school policies and procedures that inform parents and carers, staff, volunteers and governors regarding appropriate channels of communication to resolve complaints.

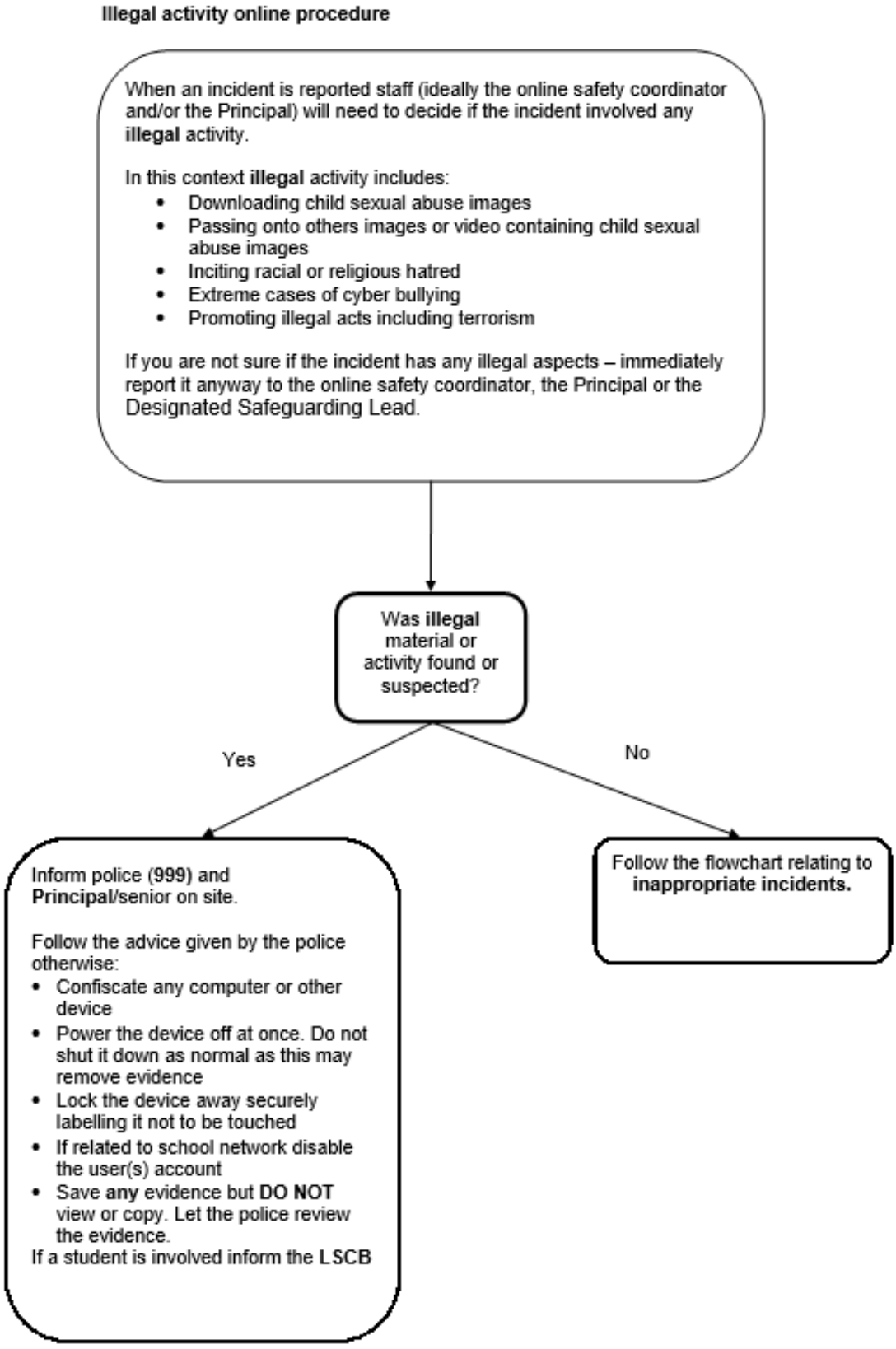
We kindly request that complaints are dealt with through official school channels rather than posting them on social networking sites.

Staff, governors, volunteers and visitors should not post malicious or fictitious comments on social networking sites, including closed groups, about any other member of the school community.

The school reserve the right to seek legal recourse should the school be named in a defamatory manner.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3:

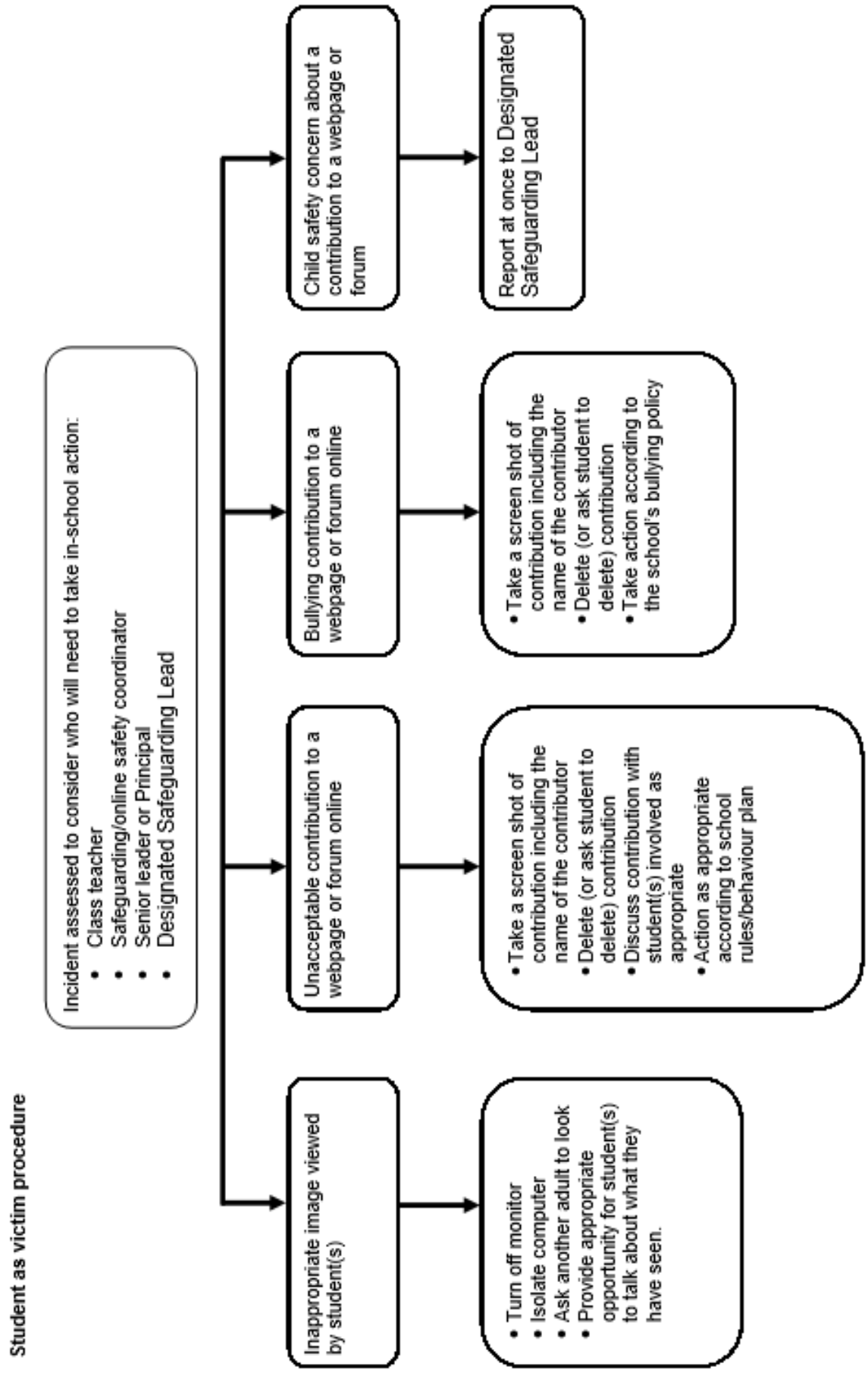
Illegal activity online procedure



Appendix 4:

Inappropriate activity online procedure
The online safety coordinator and/or Principal should:
Record in the school safeguarding or online safety incident log and keep any evidence
Incident could be:
Using another persons user name and password
Accessing content which is against school policy
Taking video without the subject's permission
Using technology to upset or bully
(in extreme cases this could be illegal – see illegal online activity procedure)
Did the incident involve a member of staff?
Yes
No
If member of staff has:
Behaved in a way that has, or may have harmed a child
Possibly committed a criminal offence
Behaved towards a child in a way which indicates s/he is unsuitable to work with children…
Contact the Designated Safeguarding Lead
Review evidence and determine if the incident is accidental or deliberate
Decide upon the appropriate course of action
Follow school disciplinary procedures (if deliberate)
If the Designated Safeguarding Lead or Principal is involved contact the Executive Director – Education or the NAS SMG
Was the student the victim or the instigator?
Student as victim
Student as instigator
Go to student as victim procedure
Review incident and identify if other students were involved
Decide appropriate action based on school rules/guidelines/behaviour plan
Inform parents/carers if serious or persistent incident
In serious incidents consider informing the Designated Safeguarding Lead as the child instigator could be at risk
Review online safety procedures/policies to develop best practice

Appendix 5:


Student as victim procedure
Incident assessed to consider who will need to take in-school action:
Class teacher
Safeguarding/online safety coordinator
Senior leader or Principal
Designated Safeguarding Lead
Inappropriate image viewed by student(s)
Turn off monitor
Isolate computer
Ask another adult to look
Provide appropriate opportunity for student(s) to talk about what they have seen.
Unacceptable contribution to a webpage or forum online
Take a screen shot of contribution including the name of the contributor
Delete (or ask student to delete) contribution
Discuss contribution with student(s) involved as appropriate
Action as appropriate according to school rules/behaviour plan
Bullying contribution to a webpage or forum online
Take a screen shot of contribution including the name of the contributor
Delete (or ask student to delete) contribution
Take action according to the school's bullying policy
Child safety concern about a contribution to a webpage or forum
Report at once to Designated Safeguarding Lead