Montsaye Community Learning Partnership

The Diocese of Peterborough

Wilbarston CEVC Primary School

Online Safety

Reviewed – September 2018

Next review – September 2019

Our Vision as a Church of England school is to deliver a caring, stimulating and enjoyable experience for all our pupils, during which pupils are expected to do their best at all times and to live out our Christian values by treating others as they would like to be treated. Pupils should leave our school with strong basic skills including communication, self-management and team-working skills, able to access the next stage of learning, be useful and caring citizens of our country with pride and awareness of our collective values and with special memories of their time at our school.

Our Mission Statement is "to learn with care, fun, faith and respect".

Ethos Statement

Recognising its historic foundation, the school will preserve and develop its religious character in accordance with the principles of the Church of England and in partnership with the Church at parish and diocesan level.

The school aims to serve its community by providing an education of the highest quality within the context of Christian belief and practice. It encourages an understanding of the meaning and significance of faith and promotes Christian values through the experiences it offers to all its pupils.

The children will gain skills, knowledge, and understanding enabling them to experience success and to realise their potential in a safe and caring environment. The children will be taught those values and attitudes which will strengthen their respect for themselves and others, enabling them to take their place in society with confidence. The way people behave towards one another plays a vital role in achieving this aim.

Aims:

For all staff to follow agreed procedure.
For parents to understand school procedure.

This policy should be read alongside the Curriculum Policy, Behaviour Policy, Anti-Bullying Policy, Safeguarding Policy and Acceptable Use Policy.

Policy Statement

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy 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 e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of online safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Designated Governor: Mrs Clare Holden

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Officer, as indicated below.

The Headteacher will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated Online Safety Officer(s) 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 Leader
Mrs Katie Curran

The Online Safety Leader will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself 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 Headteacher.
- Advise the Headteacher, governing body on all 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.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail (Appendix 1).
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.
- Deliver termly online safety assemblies to keep children up to date of risks and ways to keep safe including the age restrictions on social media.

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 Headteacher.
    - 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 Headteacher.
- Any online safety incident is reported to the Online Safety Officer (and an Online-Safety Incident report is made (Appendix 1), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the Online Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this online-safety policy are fully understood.
- http://www.childnet.com/resources/social-networking-a-guide-for-teachers-and-professionals- guidance for staff in the safe use of social media.

Mobile Technologies

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*		
Internet only	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
No network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

All Students

Online Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school. **Acceptable use policies will be signed at the beginning of each year.**

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered. Clear communication exercises will be delivered to further support parents. **Acceptable use policies will also be signed at the beginning of each year.**

Technology

Wilbarston CVCE Primary School uses a range of devices including PCs, laptops, cameras and iPads. In order to safeguard the students and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Schools Broadband software (Lightspeed) that prevents unauthorised 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 Computing Coordinator, Online Safety Teacher 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 – we use Schools Broadband software that 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.

Anti-Virus – All capable devices will have symantec endpoint anti-virus software which is updated daily. IT Support will be responsible for ensuring this is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this Online-safety and the staff Acceptable Use Policy; students upon their parents signing and returning their acceptance of the Acceptable Use 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. Staff should use @wilbarston.northants.sch.uk address for work-based emails.
Students will be given @wilbarston.northants.sch.uk to use in lessons. The children will not be able to send out external emails and a sample of their email accounts will be checked on a termly basis.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance. Photos of children will be saved into our school gallery. Parents will be reminded at school events that photos of other children are not to be placed on social media. Where photos of pupils are used children's full names will not be featured.

School website – The school website will be used to engage and collaborate with learners, and to engage with parents and the wider school community.

The following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- 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.

Blogging – In KS2, blogging websites may be used to engage learners. Teachers will have responsibility for monitoring content. There is to be no identification of students using first name and surname; first name only is to be used. Where services are "comment enabled", comments are to be set to "moderated".

Incidents - Any online safety incident is to be brought to the immediate attention of the Online Safety Teacher, or in his/her absence the Headteacher. The Online Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log (Appendix 1).

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.

Online Safety for students is embedded into the curriculum; whenever Computing 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. The Think You Know programme is used at least termly.

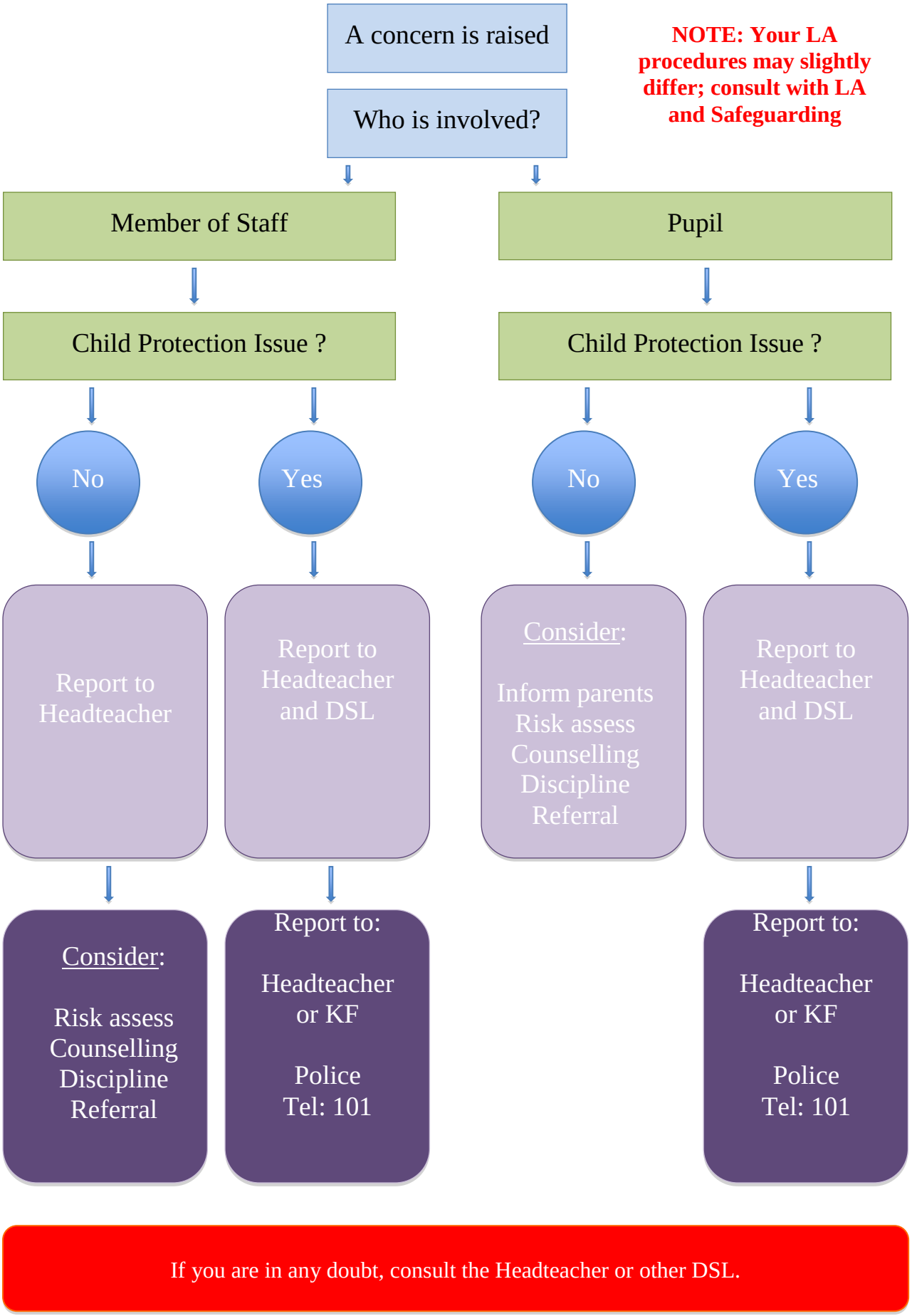
As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

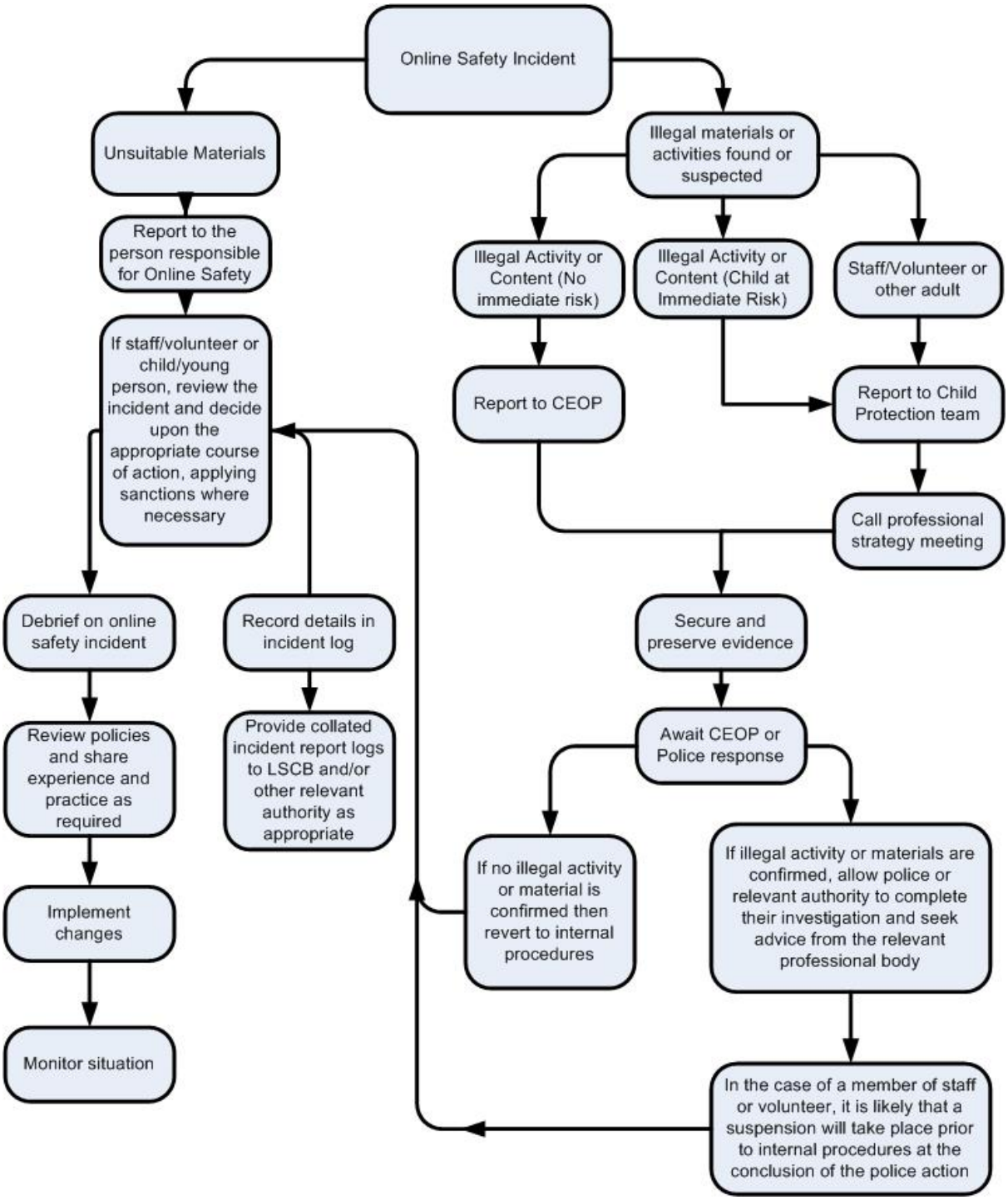
The Online Safety teacher will deliver a whole school assembly regarding internet safety at the beginning of each term.

The Online Safety teacher is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor 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.

Online Safety Officer- Simon Aston. Contact- Onlinesafety@northamptonshire.gov.uk

Inappropriate Activity Flowchart





Aims

This policy aims to ensure that:

1. Pupils, staff and parents know about cyber bullying and its consequences;
2. We have the knowledge, policies and procedures to prevent and, if necessary, to deal with cyber bullying in school or within the school community;
3. We monitor the effectiveness of our procedures.

What is cyber bullying?

• Cyber bullying includes sending or posting harmful or upsetting text, images or other messages, using the internet, mobile phones or other communication technology.

• It can take many forms, but can go even further than face to face bullying by invading home and personal space and can target one or more people.

• It can take place across age groups and target pupils, staff and others.

• It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images.

• It can include messages intended as jokes, but which have a harmful or upsetting

• effect.

Cyber bullying may be carried out in many ways, including:

• Threatening, intimidating or upsetting text messages;

• Threatening or embarrassing pictures and video clips via mobile phone cameras;

• Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;

• Threatening or bullying emails, possibly sent using a pseudonym or someone else's name;

• Menacing or upsetting responses to someone in a chat-room;

• Unpleasant messages sent during instant messaging;

• Unpleasant or defamatory information posted to blogs, personal websites and social networking sites (e.g. Facebook)

In some cases this type of bullying can be a criminal offence.

Prevention of Cyber Bullying

Understanding and information

• The Headteacher and Online Safety teacher will act, as an Online Safety Officer, to oversee the practices and procedures outlined in this policy and monitor their effectiveness.

• The Online Safety Officer will ensure that the school maintains details of agencies and resources that may assist in preventing and addressing bullying.

• Staff will be trained to identify signs of cyber bullying and will be helped to keep informed about the technologies that children commonly use.

• A Code of Advice (see Appendix 2) has been developed and will be periodically reviewed and communicated to help pupils protect themselves from being caught up in cyber bullying and to advise them on reporting any incidents.

• Pupils will be informed about cyber bullying through curricular and pastoral activities.

• Pupils and staff are expected to comply with the school's Acceptable Use Policy.

• Parents will be provided with information and advice on cyber bullying.

Practices and Procedures

• The responsibilities of the school and of pupils as set out in the Anti-Bullying Policy apply also to this policy.

• Positive use of ICT will be promoted and the Acceptable Use Policy will be kept under review as technologies develop.

• CPD and INSET may be used to help staff develop their own practices and support pupils in safe and responsible use of ICT.

• The school will encourage safe use of ICT, emphasising, for example, the importance of password security and the need to log out of accounts.

• The school will promote the message that asking for help is the right thing to do and all members of the school community will be informed how cyber bullying can be reported (class and website worry boxes).

• Confidential records will be kept of all cyber bullying incidents.

Responding to cyber bullying

Cyber bullying will generally be dealt with through the schools countering-bullying policy. A cyber bullying incident might include features different to other forms of bullying, prompting a particular response. Key differences might be:

• Impact: possibly extensive scale and scope

• Location: the anytime and anywhere nature of cyber bullying

• Anonymity: the person being bullied might not know who the perpetrator is

• Motivation: the perpetrator might not realise that his/her actions are bullying

• Evidence: the subject of the bullying will have evidence of what happened

Support for the person being bullied

As with any form of bullying, support for the individual will depend on the circumstances. Examples include:

• Emotional support and reassurance that it was right to report the incident

• Advice not to retaliate or reply, but to keep the evidence and show or give it to their parent or a member of staff

• Advice on other aspects of the code to prevent re-occurrence

• Advice on how the perpetrator might be blocked from the individual's sites or services

• Actions, where possible and appropriate, to have offending material removed

• Advice to consider changing email addresses and/or mobile phone numbers

• Discuss contacting the police in cases of suspected illegal content

Investigation

Again, the nature of any investigation will depend on the circumstances. It may include, for example,

• Review of evidence and advice to preserve it, for example by saving or printing (e.g. phone messages, texts, emails, website pages)

• Efforts to identify the perpetrator, which may include looking at the media, systems and sites used. Witnesses may have useful information.

• Contact with the Internet Watch Foundation, the police or the Northamptonshire Cyber Crime Unit.

• Requesting a pupil to reveal a message or other phone content or confiscating a phone. Staff do not have the authority to search the contents of a phone.

Working with the perpetrator

Work with the perpetrator and any sanctions will be determined on an individual basis, in accordance with the Anti-Bullying Policy, with the intention of:

• Helping the person harmed to feel safe again and be assured that the bullying will stop.

• Holding the perpetrator to account, so they recognise the harm caused and do not repeat the behaviour.

• Helping bullies to recognise the consequences of their actions and facilitating change in their attitude and behaviour.

• Demonstrating that cyber bullying, as any other form of bullying, is unacceptable and that the school has effective ways of dealing with it.

Evaluating the effectiveness of counter bullying procedures

• Members of staff will report any incidents of cyber bullying to the Head teacher.

• The Head teacher will review any serious incident within three months of the school dealing with any reported cases and will ensure that an annual review of Cyber Bullying and the Anti-Bullying procedures are carried out.

• The review will take into account comments and suggested areas for improvement from staff and students, including input from the School Council.

- Katie Curran and Mrs Green will meet to discuss issues of online safety and cyber bullying and decide upon the appropriate action to be taken.
- Where issues take place outside of school Katie Curran and/or Mrs Green will speak with the children and parents involved and decide upon the appropriate action to be taken.

Sexting

https://swgfl.org.uk/Uploads/a9/a948a63b-643b-499b-b89c-302ce8f3f739.pdf

Appendix 1- Online-Safety Concern Form

Online Safety Concerns

Date: _____

Member of staff dealing with incident: _____

Child / children incident concerns: _____

Brief outline of incident:

_____

_____

_____

_____

_____

_____

_____

_____

Actions taken following incident:

_____

_____

_____

_____

_____

Signature : _____

Please hand a copy to Katie Curran (Online Safety Co-ordinator).

If Katie Curran is not in school please give to a safeguarding lead: Andrea Green, Lucy Sheen or Karen Franklin.

Appendix 2

Cyber Safety Code

Three Steps to Safety

1. Respect other people - online and off. Don't spread rumours about people or share their secrets, including phone numbers or passwords.
2. If someone insults you online or by phone, stay calm. Ignore them, but tell someone you trust.
3. "Do as you would be done by!" Think how you would feel if you were bullied. You are responsible for your behaviour - so don't distress other people or encourage others to do so.

If you are being bullied

It is never your fault. It can be stopped and it can usually be traced.

- Don't ignore the bullying. Don't reply, but do tell someone you can trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you seem frightened or angry it will only make the person bullying you more likely to continue.

Text / video messaging

- You can turn off incoming messages for a couple of days.
- If bullying persists you can change your number (ask your mobile phone provider).
- Do not reply to abusive or worrying messages. You can report them to you mobile phone provider.

Email

- Never reply to unpleasant or unwanted messages.
- Don't accept emails or open files from people you don't know.
- Don't delete bullying emails – print them or save them as evidence in a separate folder.

Social networking sites, chatrooms and instant messaging

- Change privacy settings so you can choose who to be friends with and who can see your profile. Don't add anyone you don't know to your friend list.

• Don't use your real name in chatrooms.

• Never give out your photo or personal details, like your address, phone number or which school you go to.

Don't post any pictures or videos you wouldn't be happy for your parents or teachers to see. Once they are online they can be copied and posted in other places where you can't get rid of them.

• Keep your passwords private and don't tell anyone, not even your best friend.

• To report suspicious behaviour online and to learn more about keeping yourself safe

online visit www.thinkyouknow.co.uk

Always report bullying incidents. Not doing that allows the bully to continue.

That's not good for the victims, for those who witness the incidents or for the bully, who may need help to change their antisocial behaviour.