Wolverham Primary and Nursery School
Online Safety Policy

Online Safety: The Rationale

Online Safety encompasses the use of new technologies, internet (including social-networking) and electronic communications such as Websites, Blogs, Learning Platforms, mobile phones, Video Conferencing, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Wolverham Primary School's Online Safety policy will operate in conjunction with other policies including those for Behaviour, Safeguarding, Computing, Bullying, Curriculum, Acceptable Use, Keeping Ourselves Safe, Data Protection and Security.

Roles and Responsibilities:

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, bullying and for child protection.

The Online Safety Coordinator for Wolverham Primary School is **Mr Joseph Bullen** who works alongside Mrs Tracy Webb who is our Child Protection Coordinator.

- Our Online Safety Policy has been written by the school, building on the Cheshire Online (old e-Safety) Policy and government guidance. It has been agreed by senior management and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy was revised by: Joseph Bullen

<u>Teaching and learning</u>

Why Internet use is important:

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil and family use and will include filtering appropriate to the age of pupils.
- Pupils and families will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, both inside and outside of a school context.
- Pupils will be taught how to use the Internet safely and the dangers of disclosing personal information

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems and security will be reviewed regularly.
- Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily.
- We have adopted Cheshire West and Chester Council's security standards.
- Securus Software has been installed on all computer systems within the school and is checked every week, if not daily.
- Children will be taught about Online Safety, and parents/carers will also be informed about how to help their child stay safe at home.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Pupils will not have their own individual e-mail accounts.

Passwords

- All computers need a password to gain access, and these are changed regularly by staff through a 'forced changed' system.
- All passwords are kept safe.
- All staff email accounts have a secure password, and these are changed regularly.
- Staff memory keys are password protected by using 64-bit encryption. Sensitive data is not taken off site.

Software

- All software installed on computers is checked for age appropriate content, depending on the age of pupil accessing it.
- Pupils are taught about software that can be accessed outside of school, and the need for responsibility.

Published content and the school web site

- The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not have children's full names near the images.
- Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs.
- Parents or carers will be asked to complete giving permission for their child's photographs to be published on the school website/blog.
- An annual consent will be given to all parents/carers for the publication of children's work and photographs on the school website/blog.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Staff are not allowed to post any comments on social networking sites that relate to the school and/or children/staff. All staff sign a form to agree with these terms.
- Pupils will be taught about how to use child friendly social networking sites, and lessons will highlight the need to keep personal information safe.

Managing filtering

- The school will work with the LA, DCFS and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator who should be known to all members of the school community.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Securus Software has been installed on all computer systems within the school and is checked every week, if not daily.
- Laptops are logged in and out every time they are used so identifying any concerns is easier.

Where schools find sites or content that is inappropriate they should contact Help Desk on 01244 972126 and ask for the site to be blocked. Alternatively, Swurl can be used to block sites.

Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will not use personal equipment or non-school personal electronic accounts when contacting students. They will be issued with a school phone where contact with pupils is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Children's personal data will only be stored on teachers' laptops that have a secure password, or an encrypted USB memory stick.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- All students must read and agree to the 'Keeping Ourselves Safe Policy'.
- The school will send out Online Safety rules to parents and ask them to agree to these.
- The school will keep a central record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Within the school access to the Internet will be supervised. Lower down the school access to specific, approved on-line materials.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the local authority can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Refer to Appendix 1 for Guidance on Responding to an Incident of Concern

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to online safety.

Communications Policy

Introducing the Online Safety policy to pupils

- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- A 'Keeping Ourselves Safe' Policy is created with the Online Safety committee and reviewed each year. Every class will display this and children are made aware of the rules to stay safe and know how to report any concerns to appropriate adults in school
- Pupils are informed that network and Internet use is monitored.
- Through the development of the Online Safety scheme of work, pupils will gain knowledge and understanding of why it is important to stay safe and how to go about this.

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website/Blog.

Appendix 1

Guidance in response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

Any Online Safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to online safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Co-ordinator, the Online Safety Officer or the Police Liaison Officer.

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research**: web sites, search engines and Web browsers
- **Mobile Phones and personal digital assistants** (PDAs)
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**

What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information / images
- Hacking and security breaches

How do we respond?

The flowchart on the next page illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Child Protection Unit and Designated staff member should be consulted.

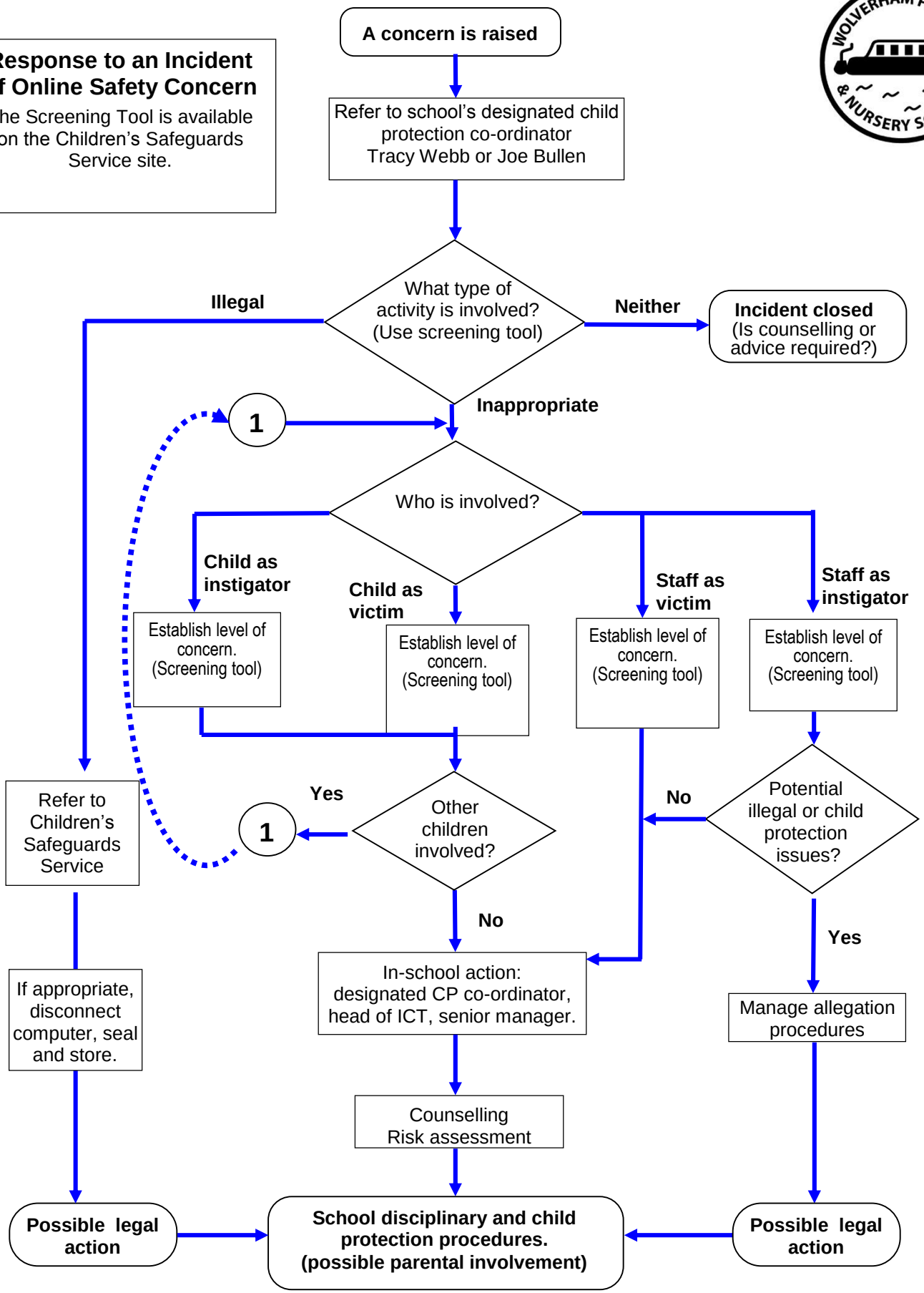
As previously stated schools should ensure that relevant policies (Acceptable Use Policy, Behaviour Policy, Bullying Policy, Discipline Policy) are referenced and are considered when dealing with the issues identified.

Updated September 2017

Review September 2018

Response to an Incident of Online Safety Concern

The Screening Tool is available on the Children's Safeguards Service site.



Screening Tool

This screening tool can be used to assist decision making in dealing with incidents of computer or e-communications misuse within your school. It can be used to inform initial action but is not a substitute for a thorough risk assessment / investigation.
This should be used alongside the Online Safety flow chart and incidents of misuse matrix.

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, please contact a member of the Child Protection Unit.

Type of incident discovered?

Sexual [ ]
Bullying [ ]
Violence [ ]
Incitement [ ]
Financial [ ]
Grooming [ ]
Other [ ]

How was the incident

Self reported [ ]
Reported by 3rd party (friends or parents) [ ]
Reported by Teacher [ ]
Other (e.g. Police, Social Services, etc) [ ]

What was their response to the incident?

Unconcerned [ ]
Curious [ ]
Distressed [ ]
Frightened [ ]
Secretive [ ]
Other [ ]

What did the incident refer to?
Answer the key questions relating to the particular incident

Child as Victim:

Content

1. What was the type of content? (Sexual, violence, racial, other) _____

2. Did anyone else see it? [ ] _____

3. Have they told anyone else about it? [ ] _____

Publishing

1. Is the child identifiable? [ ]
2. Can their location be traced/ [ ]
3. Is text or image potentially indecent or illegal? [ ]

Bullying

1. What was the type of bullying? (sexual, violent, physical, group) _____

2. Was information or images published of the child? [ ]
   (If yes, refer back to publishing section for more questions to ask)

Predation / Grooming

1. Assess the extent of the contact
   One off conversation
   [ ]
   Regular conversation
   [ ]
   Regular conversation using inappropriate or sexualised language or threats [ ]
   Attempts to breakaway
   [ ]
   Offline meeting arranged
   [ ]
   Offline meeting occurred
   [ ]
   (Consider if an offence has occurred)
2. Are the parents aware?
   [ ]

3. When did the incident occur? _____

Request for information

1. Did the child give out any personal information? [ ]

Child as Instigator:

Content

Refer to 'Child as Victim' questions on content
Refer to the matrix to assess the child's response to the content

Incitement

1. Was the child secretive about the site? [ ]
2. Did the child access the site in an isolated place? [ ]
3. Did they understand the risks of accessing this site? [ ]
4. Was their response to the site?.....

Healthy (e.g. using for research) [ ]

Problematic (looking for advice or guidance) [ ]

Harmful [ ]

(relying on site for tips, using site to communicate with likeminded individuals, the site is reinforcing /minimising potentially harmful behaviours e.g. self-harm, pro anorexia sites

Send/Publishing

1. Has an offence taken place?

[ ]

(refer to glossary for information on what constitutes an offence)

2. Were others put at risk e.g. their image / information was sent / published

[ ]

3. Was this an isolated incident or persistent?

[ ]

4. Did the instigatator have empathy for the victim?

[ ]

Interception of communications / Hacking

1. Have they placed themselves or others at risk?

[ ]

2. Has personal or financial information been stolen?

[ ]

(if yes, this constitutes a criminal offence and advice should be sought from the police)

3. Has illegal content been accessed and sent to other's computers?

[ ]

Once you have gathered the appropriate information, assess the effect of the incident on the child and identify how the child can be best supported. This may be either in school (using existing policies and resources to support children) or in certain circumstances with external help.

Staff misuse

Did the member of staff misuse the school's internal email system?

[ ]

Did the member of staff communicate with a young person inappropriately

[ ]

e.g. via text message, multimedia images.

Consider the extent of the communication

One off conversation

[ ]

Regular conversation

[ ]

Regular conversation using inappropriate or sexualised language or threats

[ ]

Attempts to breakaway

[ ]

Offline meeting arranged

[ ]

Offline meeting occurred

[ ]

(Consider if an offence has occurred)

Did the member of staff access inappropriate/ illegal material within school?

[ ]

Did the member of staff access inappropriate/ illegal material using school equipment?

[ ]

Did the member of staff access inappropriate/ illegal material using their own equipment?

[ ]

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, please contact a member of the Child Protection Unit before taking any other action.