ONLINE SAFETY POLICY

Policy reviewed November 2016

Next review November 2017

Responsibilities

The online safety co-ordinator is Mr Ronan Walsh he is responsible for leading the online safety Committee, delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote online safety within the college community. He also delivers workshops for parents/carers.

Online safety Committee

The school online safety committee is convened by the online safety officer. It will meet once per term and will invite a representative of the following groups: SLT, governors, teaching staff, admin staff, parents, pupils.

Internet use and Acceptable Use Policies (AUP's)

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role. These are sent out by the SBM each year

AUP's will be reviewed annually. All AUP's will be stored centrally in case of breaches of the online safety policy.

The AUP will form part of the first lesson of ICT for each year group.

The Prevent duty

The Prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General

advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

Internet searches for terms related to extremism
Visits to extremist websites
Use of social media to read or post extremist material
Grooming of individuals

All staff should be aware of the following

1. *DfE Prevent duty*
2. *DfE briefing note on the use of social media to encourage travel to Syria and Iraq*
3. *The Channel Panel*

The Prevent duty requires a schools monitoring and filtering systems to be fit for purpose.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used. We ask for permission from parents in our school application packs. All information regarding this is stored on SIMS.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent responses from parents when considering use of images.

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection act.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events

on social networking sites if other pupils appear in the background. Parents are reminded of this before performances and events take place.

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Mobile phones and other devices

If a pupil was to bring a mobile phone into school, this must be switched off and handed to the office where it will remain in the locked safe for the day. However, pupils are strongly encouraged not to bring mobile phones into school.

Staff are not allowed use of their mobile phones in school. If they do bring their phones into school these are to remain in lockers and not used at all during the day.

Use of e-mails

Pupils should only use e-mail addresses that have been issued by the school and the e-mail system should only be used for school related matters. Pupils are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared n. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

All users should be aware that the ICT system is filtered and monitored.

Data storage

Only encrypted USB pens are to be used in school.

Reporting

All breaches of the online safety policy need to be recorded in the ICT reporting log please see page 9. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the Designated teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require SLT intervention (eg cyberbullying) should be reported to SLT in the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (eg Ceop button, trusted adult, Childline)

Infringements and sanctions

Whenever a pupil infringes the online safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Level 1 infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to class teacher / online safety Coordinator/ confiscation of phone]

Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites
- Use of Filesharing software

- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to Class teacher/ online safety Coordinator / removal of Internet access rights for a period / confiscation of phone / contact with parent]

Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to Class teacher / online safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform SSCB/LA as appropriate

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA online safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to online safety incidents that take place out of school if they are related to school.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Social networking

Pupils are not permitted to use social networking sites within school.

Education

Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

a). A planned, broad and progressive online safety education programme that is fully embedded for all children , in all aspects of the curriculum, in all years.
b). Regularly auditing, review and revision of the ICT curriculum
c). Online safety resources that are varied and appropriate and use new technologies to deliver online safety messages in an engaging and relevant manner
d). Opportunities for pupils to be involved in online safety education e.g. through peer mentoring, online safety committee, parent presentations etc

Additionally,

a). Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
b). There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
c). The school actively provides systematic opportunities for pupils / pupils to develop the skills of safe and discriminating on-line behaviour
d). Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

a). A planned programme of formal online safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent duty.
b). Online safety training is an integral part of Child Protection / Safeguarding training and vice versa
c). An audit of online safety training needs is carried out regularly and is addressed
d). All staff have an up to date awareness of online safety matters, the current school online safety policy and practices and child protection / safeguarding procedures
e). All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policy

f). Staff are encouraged to undertake additional online safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) Online safety Certificate
g). The culture of the school ensures that staff support each other in sharing knowledge and good practice about online safety
h). The school takes every opportunity to research and understand good practice that is taking place in other schools
i). Governors are offered the opportunity to undertake training.

Parents and the wider community

There is a planned programme of online safety sessions for parents, carers, etc. This is planned, monitored and reviewed by the online safety co-ordinator with input from the online safety committee.

Monitoring and reporting

a). The school network provides a level of filtering and monitoring that supports safeguarding.

b). The impact of the online safety policy and practice is monitored through the review / audit of online safety incident logs, behaviour / bullying logs, surveys of staff, pupils /pupils, parents / carers

c). The records are reviewed / audited and reported to:

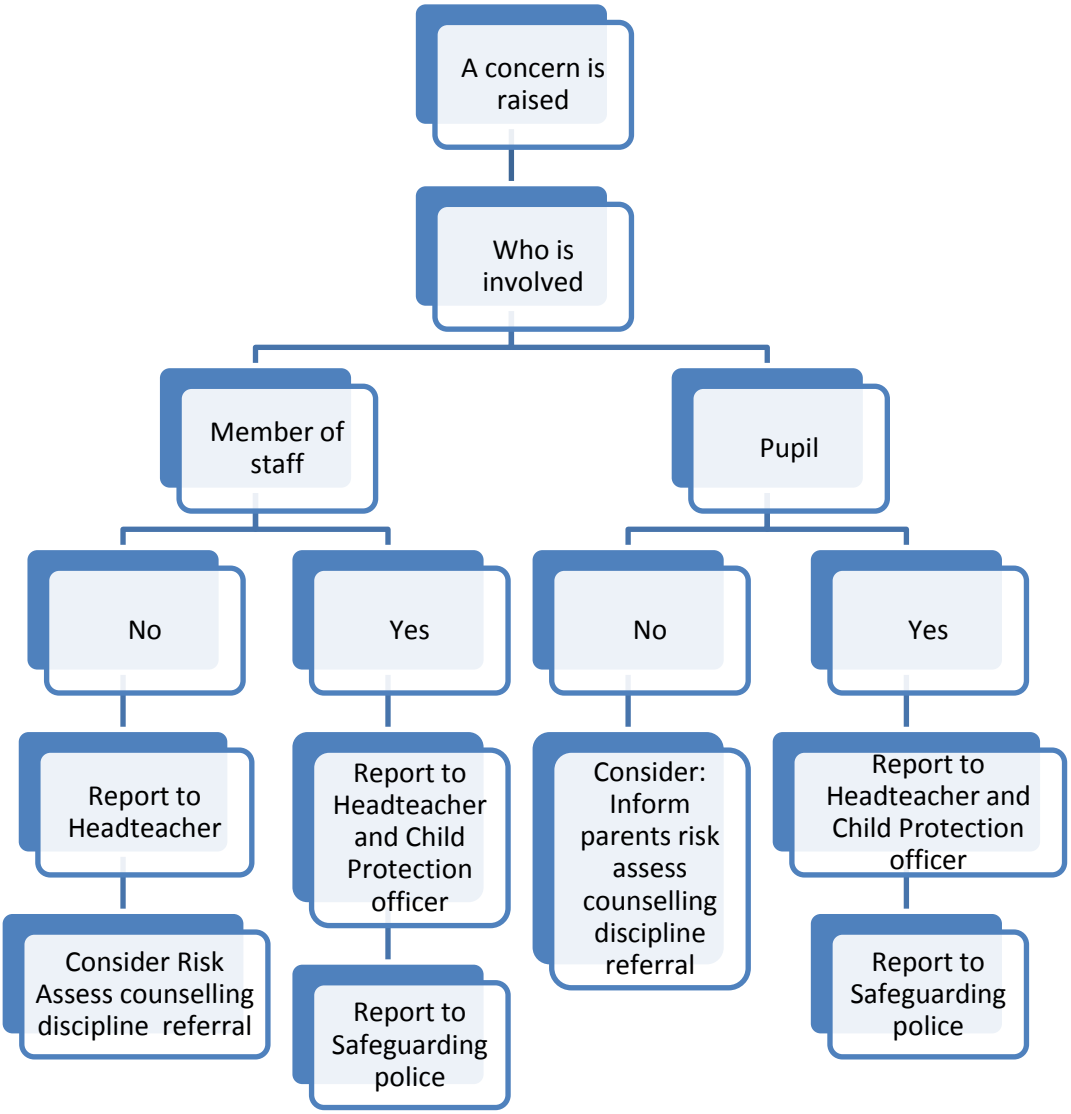
- the school's senior leaders
- Governors
- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Children Board (SSCB) Online safety Sub Committee (where necessary)

d). The school action plan indicates any planned action based on the above.

Online safety Incident Log

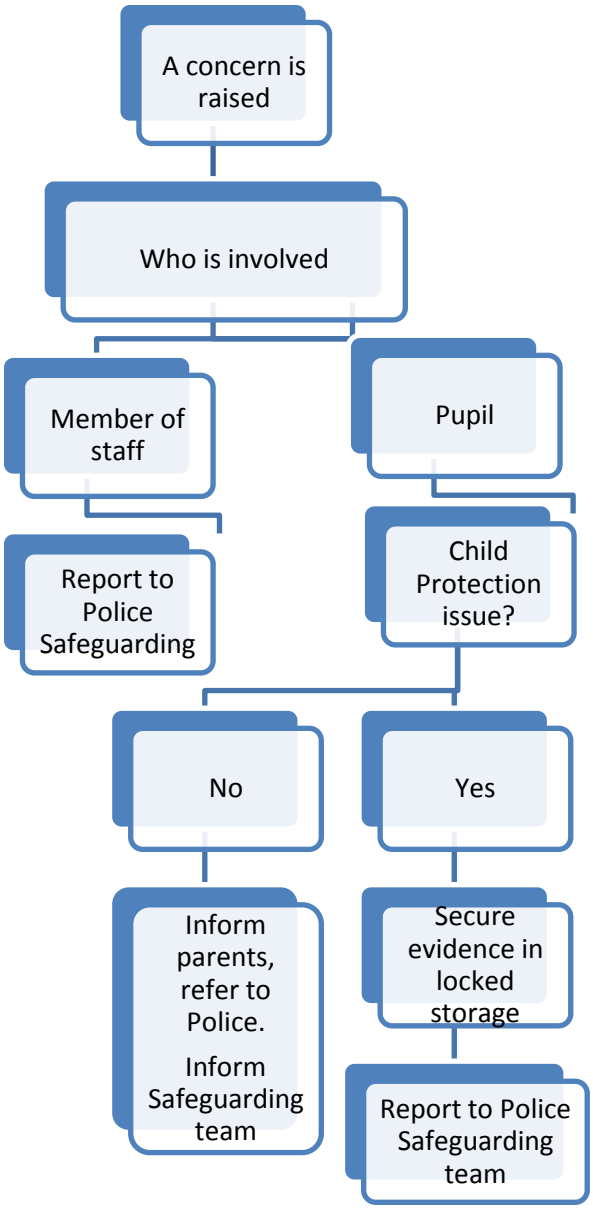
Number:	Reported by(name of staff member)	Reported To:(e.g. Head, Deputy)
	When:	When:
Incident Description:(Describe what happened, involving which children and/or staff, and what action was taken)		
Review Date:		
Result of Review:		
Signature of Headteacher:		Date:
Signature of Governor:		Date:

Inappropriate activity flowchart



<u>If you are in any doubt consult the Headteacher, Child Protection Officer or Safeguarding team</u>

Illegal activity flowchart



<u>NEVER investigate</u>

<u>NEVER show to others for your own assurance</u>

<u>DO NOT let others handle evidence, this is for the Police only</u>