Seamer and Irton CP School

Online Safety Policy

Policy name	**Online Safety Policy**
Frequency of review	Annual
Governor lead	Matthew Millington
Lead member of staff	Hannah Griffiths
Reviewed on	18 March 2021
Reviewed by	Governing Board
Next review	March 2022

Introduction

This policy has been prepared by the Online safety co-ordinator and has been agreed by the Headteacher, Governing Body and all members of the school's teaching staff.

Our aims are to ensure that all pupils:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world, including the need to avoid undesirable material
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working
- will be able to identify potential online risks and know what to do should such dangers arise
- will use technologies safely.

In order to achieve these goals, the whole school community have a responsibility in educating the pupils and minimising the unavoidable risks that pupils face online.

The following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Governing Body:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving information about any online safety incidents which may occur. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- Review/monitoring of filtering systems
- reporting at relevant Governors' meeting

Headteacher and SLT:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher and the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (See Appendix 2 and relevant Local Authority HR).
- The Headteacher and Senior Leaders 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 Headteacher and Senior Leadership Team will receive details of all online Safety issues which may arise.

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 / 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
- liaises with network managers
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets with the Online Safety Governor to discuss current issues, review incident logs and filtering
- attends relevant Governors meetings
- reports any online safety issues to the Senior Leadership Team

Network Manager and Firewall provider:

The school's internet access is filtered by our internet service provider EXA, using their filtering service, SurfProtect (https://surfprotect.co.uk/pdf/DfE_Guidelines.pdf). In addition, the school will protect the computer network infrastructure using the antivirus software, ESET NOD32 which is managed by our network managers, SMD Solutions.

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet and remote access is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Online Safety Coordinator for investigation
- that monitoring software / systems are implemented and regularly updated

Teaching and Support Staff

Teaching and support staff have a key role in educating pupils about potential online dangers and how to minimise online risks. Teaching and support staff should ensure that the computing and PSHE schemes of work are followed which each contain online safety objectives; however, staff should also adapt their lessons to the needs of their pupils and to address the ever changing, and increasing online risks faced by the pupils.

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 practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- pupils in their care understand and follow the Online Safety Policy and acceptable use policies
- they report any suspected misuse or problem to the Headteacher or a member of the Senior Leadership team, or Online Safety Coordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- Photographs published on the school website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that themselves
- in lessons where pupils are carrying out independent research, pupils must be reminded about the pupil AUP, in particular, what to do if they come across inappropriate content.

Pupils:

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand what good practice is when using mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- 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

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will communicate these issues to parents to help them understand these issues. Parents and carers will be encouraged to support the school in promoting good online safety practice:

- Read and sign the acceptable use policy for parents and pupils, and encourage their children to adhere to them.

- Discuss online safety issues with their children, support the school in its online safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.
- All new parents will be asked to sign the parent/carer AUP which outlines key online safety expectations.

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign a staff/volunteer AUP before being provided with access to school systems. The AUP should be discussed with any community users to ensure that they are fully aware and understand the points detailed in the AUP.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

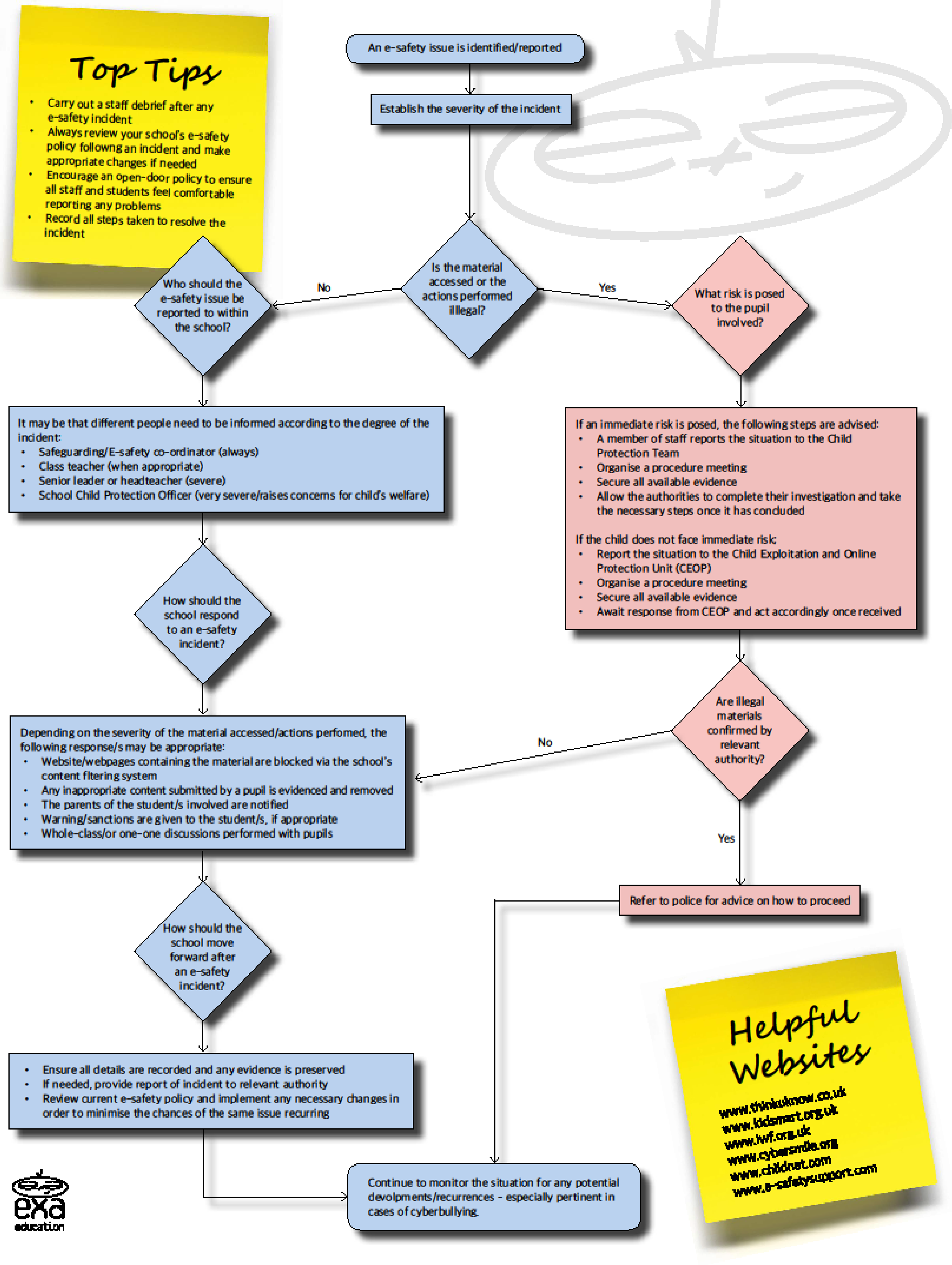
In all instances, where information, messages or images may later be used as evidence, the device should be isolated as well as practicably possible and only the monitor should be switched off, or the screen closed to 45degrees if using a laptop. All incidents should be reported to the headteacher, the online safety coordinator or a member of the senior leadership team immediately, who will follow the incident flowchart (Appendix 1).

Instances of staff internet misuse or suspected misuse should be reported to, and dealt with by, the Headteacher.

Appendix 1

Guidance on Responding to E-Safety Incidents

In the event of an e-safety incident, a clear and defined action document is invaluable to a school. This guidance should be available to all members of staff, ensuring that the correct steps are followed and the right persons/authorities are notified. Although the specific procedures may vary for each school, the flowchart below is a helpful starting point in understanding how to respond to an e-safety incident.



Top Tips

- Carry out a staff debrief after any e-safety incident
- Always review your school's e-safety policy followng an incident and make appropriate changes if needed
- Encourage an open-door policy to ensure all staff and students feel comfortable reporting any problems
- Record all steps taken to resolve the incident

An e-safety issue is identified/reported

Establish the severity of the incident

Is the material accessed or the actions performed illegal?

No

Yes

Who should the e-safety issue be reported to within the school?

What risk is posed to the pupil involved?

It may be that different people need to be informed according to the degree of the incident:

- Safeguarding/E-safety co-ordinator (always)
- Class teacher (when appropriate)
- Senior leader or headteacher (severe)
- School Child Protection Officer (very severe/raises concerns for child's welfare)

If an immediate risk is posed, the following steps are advised:

- A member of staff reports the situation to the Child Protection Team
- Organise a procedure meeting
- Secure all available evidence
- Allow the authorities to complete their investigation and take the necessary steps once it has concluded

If the child does not face immediate risk:

- Report the situation to the Child Exploitation and Online Protection Unit (CEOP)
- Organise a procedure meeting
- Secure all available evidence
- Await response from CEOP and act accordingly once received

How should the school respond to an e-safety incident?

Are illegal materials confirmed by relevant authority?

No

Depending on the severity of the material accessed/actions perfomed, the following response/s may be appropriate:

- Website/webpages containing the material are blocked via the school's content filtering system
- Any inappropriate content submitted by a pupil is evidenced and removed
- The parents of the student/s involved are notified
- Warning/sanctions are given to the student/s, if appropriate
- Whole-class/or one-one discussions performed with pupils

Yes

Refer to police for advice on how to proceed

How should the school move forward after an e-safety incident?

Helpful Websites

www.thinkuknow.co.uk
www.kidsmart.org.uk
www.iwf.org.uk
www.cybersmile.org
www.childnet.com
www.e-safetysupport.com

- Ensure all details are recorded and any evidence is preserved
- If needed, provide report of incident to relevant authority
- Review current e-safety policy and implement any necessary changes in order to minimise the chances of the same issue recurring

Continue to monitor the situation for any potential devlopments/recurrences – especially pertinent in cases of cyberbullying.

exa education

Appendix 2

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow the school's online safety policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action

- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism