Elloughton Primary School
E-Safety Policy
January 2016

1. OVERVIEW

This eSafety policy was created by the senior management Team at Elloughton Primary School.
The policy was completed on: **December 2011**
The policy was approved by the governing body on: **29th February 2012**
The policy is due for review no later than: **1st March 2017**
The eSafety Coordinator is: **Mrs Woodend**

2. INTRODUCTION

At Elloughton Primary School we fully recognise, acknowledge and embrace the importance and benefits of a connected world. The opportunities for learning created by providing access to such a world are limitless, and must therefore become part of day to day teaching and learning in school.

Being part of the internet community, as well as providing the aforementioned opportunities, also opens up the possibilities of exposure to dangers which would otherwise not be present, for example: access to inappropriate materials, contact with potentially dangerous strangers, "cyber" bullying and identity theft. It must therefore be the role of the school to ensure that such risks are minimised, and, more importantly, that children are provided with the knowledge , skills and attitude necessary to become positive, safe and healthy on-line citizens.

3. RESPONSIBILITIES OF THE SCHOOL COMMUNITY

We believe that eSafety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of Management Team

- Develop and promote an eSafety culture within the school community.
- Support the eSafety Coordinator in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to eSafety effectively.
- Receive and regularly review eSafety incident logs and be aware of the procedure to be followed should an eSafety incident occur in school.
- Take ultimate responsibility for the eSafety of the school community.

Responsibilities of the eSafety Coordinator

- Promote awareness and commitment to eSafety throughout the school.
- Be the first point of contact in school on all eSafety matters.
- Lead the eSafety group.
- Create and maintain eSafety policies and procedures.
- Develop an understanding of current eSafety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in eSafety issues.
- Ensure that eSafety education is embedded across the curriculum.
- Ensure that eSafety is promoted to parents and carers.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on eSafety issues to the eSafety group and SMT as appropriate.
- Ensure that an eSafety log is kept up to date.

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy.
- Develop and maintain and awareness of current eSafety issues and guidance.
- Model safe and responsible behaviour in your own use of technology.
- Embed eSafety messages in learning activities involving technology.
- Be aware of what to do if an eSafety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Technical Staff

- Read, understand, contribute and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school ICT system.
- Report any eSafety related issues that come to your attention to the eSafety Coordinator.
- Develop and maintain an awareness of current eSafety issues, legislation and guidance relevant to your work.
- Liaise with the local authority and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

- Read, understand and adhere to the school pupil Acceptable Use Policy.
- Help and support the school in creating eSafety policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies in school and at home.
- Take responsibility for your own and each others' safe and responsible use of technology in school and at home,
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.

- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss eSafety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support your school in promoting eSafety.
- Read, understand and promote the school pupil Acceptable Use Policy with your children.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that your children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss eSafety concerns with your children, show an interest in how they are using technology and encourage them to behave safely and responsible when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's eSafety policies and guidance.
- Develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- Develop an overview of how the school ICT infrastructure provides safe access to the internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the eSafety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety activities.
- Ensure appropriate funding and resources are available for the school to implement their eSafety strategy.

4 LEARNING AND TEACHING

- We believe that the key to developing safe and responsible behaviours on line, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in pupil's lives not just in school but outside as well, and we believe we have a duty to help prepare our children's to safely benefit from the opportunities the internet brings.
- We will provide a series of specific eSafety related lessons in every year group as part of the ICT curriculum/ PSCHE curriculum and other lessons.
- We will celebrate and promote eSafety through Safer Internet Day each year and celebration of our learning on the school website.
- We will discuss, remind or raise relevant eSafety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need for respect and acknowledge ownership of digital materials.

- We will remind pupils about their responsibilities through an end-user AUP which every pupil will sign and will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

5. HOW PARENTS AND CARERS WILL BE INVOLVED.

We believe that it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Hold parent meeting on eSafety / include eSafety as part of parent meeting.
- Include useful links and advice on eSafety regularly in Newsletters and on the website.
- Include a section on eSafety in the school handbook.

6. MANAGING ICT SYSTEMS AND ACCESS

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept updated as appropriate.
- The school will agree which users should and should not have internet access, and the appropriate level of access and supervision they should receive.
- All users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- At Foundation stage/ Key Stage one / Key Stage two pupils will access the internet using an individual log on which will be their name and password. Internet access will be supervised AT ALL TIMES by a member of staff.
- Members of staff will access the internet using an individual log on. They will ensure they log out after each session, and not allow pupils to access the internet through their log on. They will abide by the school AUP at all times.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. Headteacher and member of technical support.
- The wireless network in school is encrypted to reduce the risk of unauthorised access.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will occur.
- The school will regularly audit ICT use to establish if the eSafety policy is adequate and that implementation of the eSafety policy is appropriate. We will regularly review our internet access provision

7. FILTERING INTERNET ACCESS

- The school uses a filtered internet service. The filtering is provided through **Smoothwall and Primary Tec.**
- If users discover a website with an inappropriate content, this should be reported immediately to the eSafety Coordinator.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafety Coordinator. The school will report this to appropriate agencies including the filtering provider.
- The school will regularly review the filtering and the security systems to ensure they meet the needs of all users.

8. LEARNING TECHNOLOGIES IN SCHOOL

	Pupils	Staff
Personal mobile phones in school	No	Yes
Mobile phones used in lessons	No	No
Mobile phones used outside of lessons	No	Yes *
Taking photographs or videos on personal equipment	No	No
Taking photographs or videos on school devices.	Yes	Yes
Use of hand held devices such as PDAs, MP3 players or personal gaming consoles.	Yes	Yes
Use of personal emails addresses in school	No	Yes
Use of school email address for personal correspondence	Yes	With permission
Use of online chat rooms	No	No
Use of blogs, wikis, podcasts or social networking sites.	Yes	Yes as controlled by filtering
Use of video conferencing / online video meetings	supervised	Yes

* Phones are to be used by staff to make and receive calls and text messages when there are no children around. The phone is to be on silent and in a bag during lessons. Staff are not allowed to show photos/play music from their phone to pupils. Staff cannot allow any contact with pupils and their own personal phones.

9. USING EMAIL

- Pupils should use approved email accounts allocated to them by the school, and be aware that their use of the email system will be monitored and checked.
- Staff can choose to use school email address or their own email address. Any communication will be forwarded to school email only.
- Pupils will be reminded when using email about the need to send polite and responsible messages, about the dangers of revealing personal information, opening emails from unknown sender and viewing/opening attachments.
- Pupils are not permitted to access personal email accounts during school.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

Any inappropriate use of the school email system or the receipt of any inappropriate messages by the user should be reported to a member of staff immediately.

10. USING IMAGES, VIDEOS AND SOUND

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, videos and sound. We will remind them of the risks of inappropriate use of digital images, video and sound on their online activities both at school and at home.
- Digital images, video and sound will be created using equipment provided by the school or by staff who have signed the staff AUP; images of children will not be stored on personally owned computer equipment.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants: images and video will be of appropriate activities and participants will be in appropriate dress: full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff / pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published on line.

11. USING VIDEO CONFERENCING AND OTHER ONLINE VIDEO MEETINGS AND BLOGS

- In the near future we will start to use blogs or podcasts to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However we will ensure that staff and pupils take part in these activities in a safe and responsible manner.
- In the near future we might use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear them. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner.
- All video conferencing activity will be supervised by a suitable member of staff.
- Pupils will not operate video conferencing equipment, or answer calls, without the permission from the supervising member of staff.
- Video conferencing equipment will be switched off and secured when not in use / online meeting rooms will be closed and logged off when not in use.
- Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
- Video conferencing should not take place off school premises without the permission of the Headteacher.
- Parental permission will be sought before taking part in video conferences.
- Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be available outside of the school.

12. USING MOBILE PHONES

- Pupils' personal mobile phones are not allowed in school. (Older children who have them for safety going to and from school must hand them in as soon as they arrive on the playground.)
- Staff usually prefer to carry their own mobile phones on school visits, rather than a "school mobile". Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or personal details may be revealed to a parent or pupil.

13. USING NEW TECHNOLOGY

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from a safety point of view.
- We will regularly amend the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafety risk.

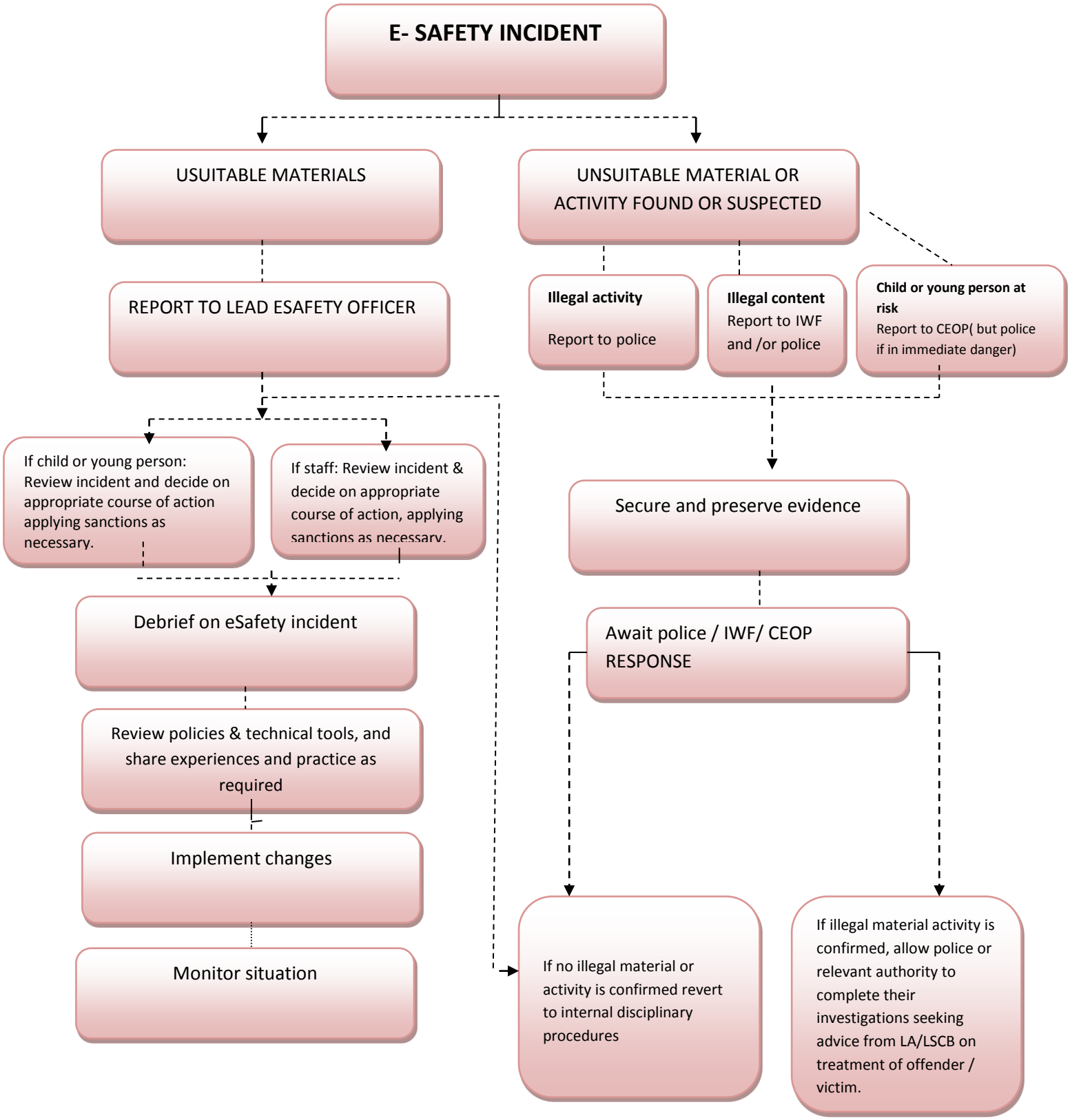
14.

- We will ensure personal data personal data is recorded, processed, transferred and made available to the Data Protection Act 1998.
- Staff will ensure they properly log off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive material from the school premises without permission from the Headteacher. Any data, which is impractical to ensure is kept in school, (e.g. reports) will be removed in password / encrypted format.
-

15. SCHOOL WEBSITE AND OTHER ONLINE CONTENT PUBLISHED BY THE SCHOOL.

- The school website will not include the personal details, including individual email addresses or full name of staff and pupils.
- A generic contact email address will be used for all enquiries received through the school website.
- All content included on a school website will be approved by the Headteacher before publication.
- Photographs of children will only appear on the website with parental permission.
- Staff and pupils should not post school related content on any external website without seeking permission first. No school related content may be posted on any social networking site.

Dealing with ESafety incidents



CYBER BULLYING INCIDENT FORM

Report Number _____ Date of report_____

Person making report

Name:		Student Staff (circle one)
Age: Sex:	School:	Year group:

Victims Information

Name:		Student Staff (circle one)
Age: Sex:	School:	Year group:

Offender 1 Information

Name:		Student Staff (circle one)
Age: Sex:	School:	Year group:

Offender 2 information

Name:		Student Staff (circle one)
Age: Sex:	School:	Year group:

Bystander/ witness information

Name:		Student Staff (circle one)
Age: Sex:	School:	Year group:

Name:		Student Staff (circle one)
Age: Sex:	School:	Year group:

Name:		Student Staff (circle one)
Age: Sex:	School:	Year group:

Location of Incident

Description of incident

Did the incident involve any of the following? :

	YES (√)	NO (√)
Threat to someone's physical safety		
Sexual harassment		
Discrimination based on race, gender, or sexual orientation. (*please note a separate racial discrimination form will need to be completed)*		
Repeated cyber bullying after previous intervention		
Image or video or audio recording of harassment		
Other noticeable features		

Tick all that apply

	YES (√)	NO (√)
Email		
Text messaging		
Video conferencing		
Social network site (please name)		

Did the incident result in a substantial disruption of the school YES/NO ** Delete as appropriate*

If yes please give details below:

Attach printouts of all evidence and additional sheets with statements by individuals listed.

Tick all people informed:

Class teacher	☐	Headteacher / Deputy	☐
ESafety Coordinator	☐	Police	☐
ITC Support services	☐	Parents	☐

Description of Action Plan:

What sanctions are being put in place and what steps are taken to ensure behaviour does not continue?

What additional consequences will be applied if offender fails to comply with action plan?

Comments by Headteacher

Any further information

Witness Statement

Name _____

Signature _____