E-Safety Policy and Acceptable Use of ICT

Non Statutory Policy

To be reviewed annually

Ratified by FGB – 16th September 2019

Review date – 16th September 2020

1. Introduction

At Northborough Primary School we understand the responsibility we have to educate our pupils on e-safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Northborough Primary School has a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive e-safety programme for pupils, staff and parents.

This policy is to be read in conjunction with all other policies particularly: Behaviour Policy, Safeguarding Policy and Child Protection Policy, Code of Conduct policy, and Equal Opportunities Policy.

2. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in Northborough Primary School. All staff on the Child Protection team have received CEOP (Child Exploitation and Online Protection) training.

Mr S Mallott (Headteacher) has overall responsibility. With Mrs B Rich as Deputy Safeguarding Lead, Mrs S Jackson and Mrs H Hussey these are named staff for children to report any concerns.

It is the role of these staff members to keep abreast of current issues and guidance through organisations such as Enfield LA, Becta, CEOP (Child Exploitation and Online Protection), and Child Net. The Head teacher ensures Senior Management and Governors are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school safety procedures.

All staff should be familiar with the school's policy including:

• safe use of e-mail

• safe use of the Internet

• safe use of the school network, equipment and data

• safe use of digital images and digital technologies, such as mobile phones and digital cameras

• publication of pupil information/photographs on the school website

• procedures in the event of misuse of technology by any member of the school community (see appendices)

• their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school (see appendix 1 for staff acceptable use agreement).

Managing the school e-safety messages

• We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.

• The e-safety policy will be shared with new staff, including the acceptable use policy as part of their induction.

• E-safety posters will be prominently displayed.

3. Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new ways to promote e-safety.

• We provide opportunities within a range of curriculum areas to teach about Esafety.

• Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.

• Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the ICT curriculum.

• We regularly distribute questionnaires to children to monitor their understanding of e-safety. Please see Appendix 11.

• Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.

• Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

4. Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education as well as a potential risk to young people.

Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.

Staff will preview any recommended sites before use.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety co-ordinator and an email sent to the network manager so that they can block the site.

It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Any changes to filtering must be authorised by a member of the senior leadership team.

5. Security and Data Protection

The school and all staff members comply with the Data Protection Act 1998. Personal data will be recorded, processed, transferred and made available according to the act. Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have secure passwords which are not shared with anyone. All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy.

6. E-Safety Complaints/Incidents

As a school we take all precautions to ensure e-safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. Complaints should be made to the Headteacher. Incidents should be logged and the flowchart for managing an e-safety incident is to be followed. It is important that the school work in partnership with pupils and parents to educate them about Cyber bullying and children, staff and families need to know what to do if they or anyone they know are a victim of Cyber bullying. All bullying incidents should be recorded and investigated via the incident log form (Appendix 6).

7. Review of Policy

There are on-going opportunities for staff, children and families to discuss e-safety concerns with class teachers or Designated Child Protection officers. This policy needs to be reviewed every 12 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or any guidance or orders are updated.

Appendix

1. Primary Pupil Acceptable Use of ICT Agreement/E-Safety Rules
2. Parent Internet use form/letter
3. Staff, Governor and Visitor Acceptable Use Agreement
4. Flow chart for managing an e-safety incident not involving any illegal activity
5. Flow chart for managing an e-safety incident involving illegal activity
6. E-Safety Incident Log
7. Advice for children on Cyber bullying – Enfield document
8. Advice for parents on Cyber bullying – Enfield document
9. KS1 Internet tips
10. KS2 Internet tips
11. E-safety questionnaires

Appendix 1

NORTHBOROUGH PRIMARY SCHOOL

Primary Pupil Acceptable Use of ICT

Agreement/E-Safety Rules

- I will only use ICT in school for school purposes.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will not bring software, CDs or ICT equipment into school without permission.
- I will only use the Internet after being given permission from a teacher.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not use technology in school time to contact other people, or access online chatrooms.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my eSafety.

Appendix 2

NORTHBOROUGH PRIMARY SCHOOL
Church Street
Northborough
Peterborough
office@Northborough.peterborough.sch.uk

Headteacher: Mr S. Mallott

Dear Parents/Carers,

ICT, including the internet, e-mail and mobile technologies, has become an important part of learning in schools. We expect all children to be safe and responsible when using any ICT.

Please read and discuss with your child the E-Safety rules overleaf by accessing ICT in school you are agreeing to the following. If you have any concerns or would like some explanation please contact your child's class teacher.

This Acceptable Use of ICT Agreement is a summary of our E-Safety Policy which

is available in full on our website or as a hard copy in our Office/Reception.

Yours sincerely,

Mr Mallott

Headteacher

Parent's/Carer's Internet Access – By accessing the ICT in school you agree to the following:

I have read and understood the school rules for Acceptable Use of ICT. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

Appendix 3

Northborough Primary School
Acceptable Use of ICT Agreement
Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr S Mallott, Headteacher or a member of the Child Protection team.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on Integris) is kept secure
- and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed
- remotely when authorised by the Head or Governing Body.
- I will not use or install any hardware (including USB sticks) or software without permission from the e-safety co-ordinators.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or
- staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

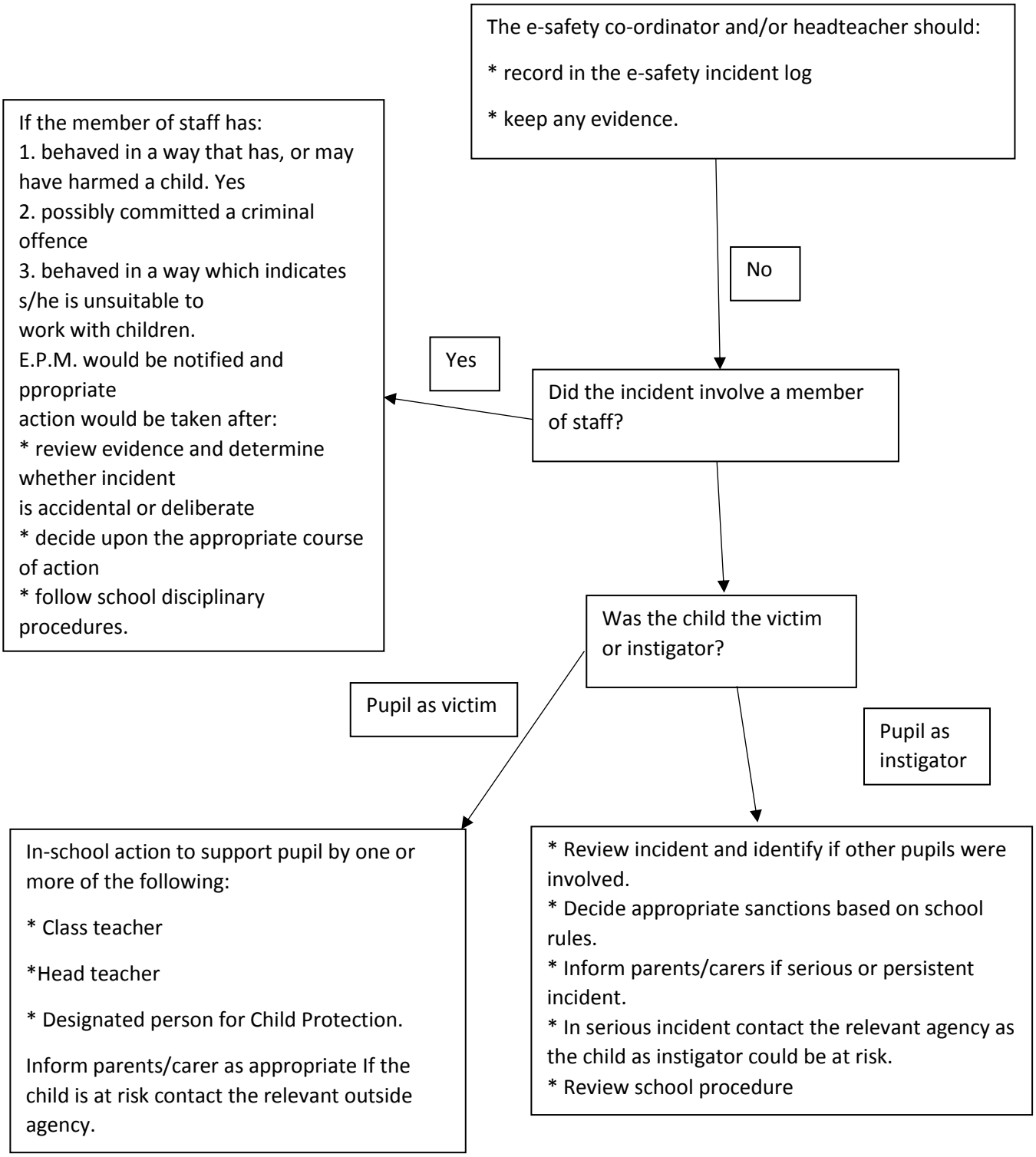
Full Name …….. (printed)

Job title: ……..

Flowchart for Managing an e-safety incident not involving any illegal activity

Incidents not involving any illegal activity, such as:

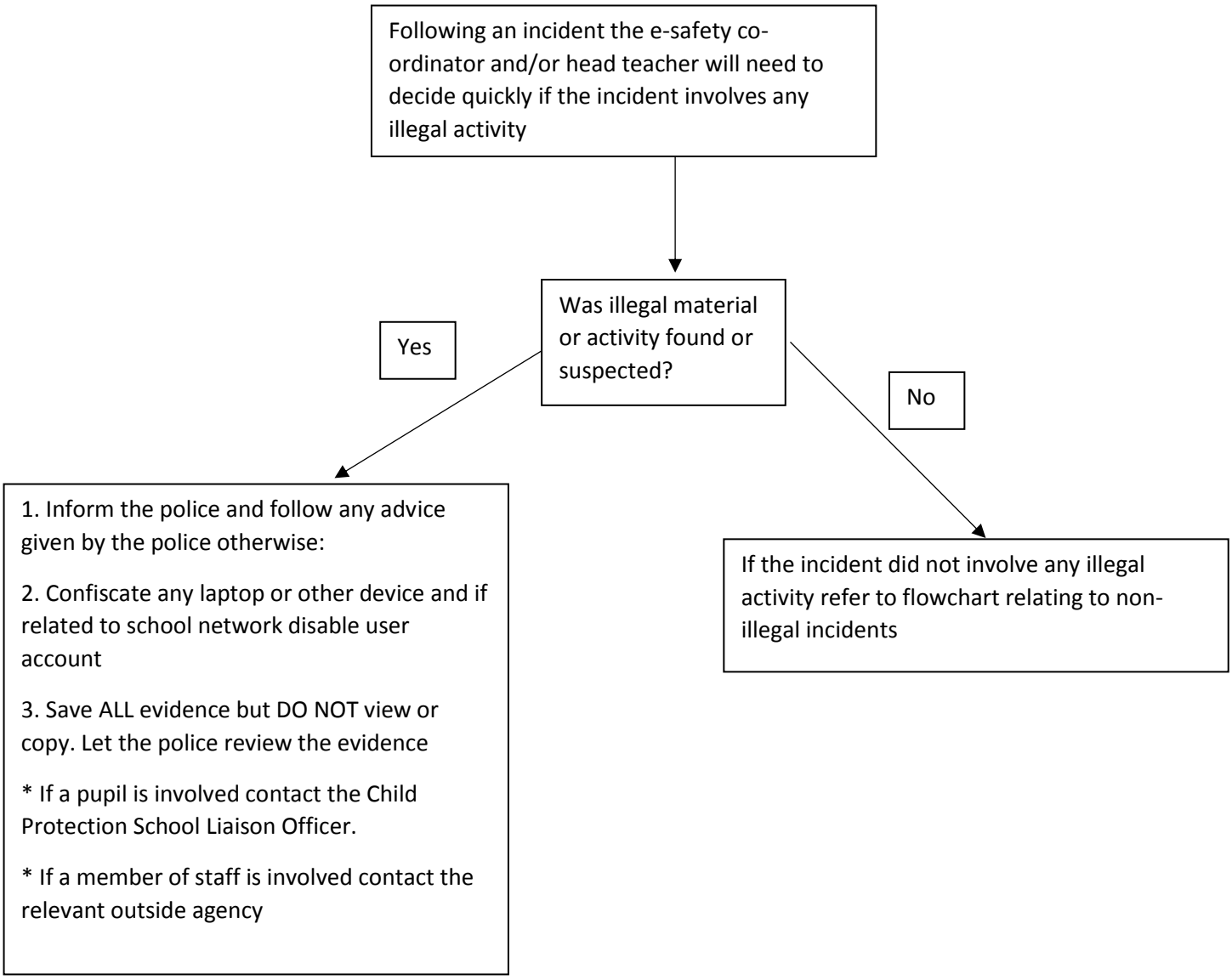
- using another person's user name and password
- accessing websites which are against school policy
- using a mobile phone to take video during a lesson
- using the technology to upset or bully (in extreme cases this could be illegal)



Flowchart for Managing an e-safety incident involving illegal activity

Illegal means something against the law, such as:

- downloading child pornography
- passing onto others images or video containing child pornography
- inciting racial or religious hatred
- promoting illegal acts



Appendix 6

Northborough Primary School E-Safety Incident Log

Details of ALL e-safety incidents to be recorded in the Incident Log by the safety co-ordinator. This incident log will be monitored termly by the e-safety coordinator and Head teacher.

Date & time	Name of pupil or staff	Male or Female	Class and Details or computer/device	Details of incident (including evidence)	Actions and reasons

Appendix 7

Advice for Children on Cyber-bullying

If you're being bullied by phone or the Internet

- Remember, bullying is never your fault. It can be stopped and it can usually be traced.
- Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.
- Don't give out your personal details online - if you're in a chatroom, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.
- Keep and save any bullying emails, text messages or images. Then you can show them to a parent or teacher as evidence.
- If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.

There's plenty of online advice on how to react to cyberbullying. For example, www.kidscape.org and www.wiredsafety.org have some useful tips:

Text/video messaging

You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number.

To find out how to do this, visit www.wiredsafety.org.

- If the bullying persists, you can change your phone number. Ask your mobile service provider.
- Don't reply to abusive or worrying text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.
- Don't delete messages from cyberbullies. You don't have to read them, but you should keep them as evidence.

Text harassment is a crime. If the calls are simply annoying, tell a teacher, parent or carer. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received.

Phone calls

If you get an abusive or silent phone call, don't hang up immediately.

Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise they can't get you rattled, callers usually get bored and stop bothering you.

- Don't give out personal details such as your phone number to just anyone. And never leave your phone lying around. When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not. You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it.

- And do not leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again. Almost all calls nowadays can be traced. If the problem continues, think about changing your phone number. If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too.

Emails

- Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.
- Keep the emails as evidence. And tell an adult about them.
- Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. abuse@hotmail.com
- Never reply to someone you don't know, even if there's an option to 'unsubscribe'. Replying simply confirms your email address as a real one.

Web bullying

If the bullying is on a website (e.g. Bebo) tell a teacher or parent, just as you would if the bullying was face-to-face – even if you don't actually know the bully's identity.

Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging

- Never give out your name, address, phone number, school name or password online.
- It's a good idea to use a nickname. And don't give out photos of yourself.
- Don't accept emails or open files from people you don't know.
- Remember it might not just be people your own age in a chatroom.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.
- Think carefully about what you write; don't leave yourself open to bullying.
- Don't ever give out passwords to your mobile or email account.

Three steps to stay out of harm's way

1. Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.
2. If someone insults you online or by phone, stay calm – and ignore them.
3. Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else.

Anti-Bullying & Cyber bullying questionnaire KS1

Class…… No. of pupils taking part ……

1. Does the word bullying mean;

Someone is unkind to you once……

Someone is unkind to you more than once…….

2. If you were unhappy at school, who would you tell?

……

How many said they did not know who to tell?.....

3. How many children did not know about the E-Safety rules? …….....

4. How many children use the internet at home?

……

5. How many of those children use the internet;

(a) Alone…….

(b) With an adult……

6. If you were out with your family and you got separated from them, what would you do?

……

……

(Please explain the importance of knowing either their address, post code or a contact number)

Anti-Bullying & Cyber bullying KS2 Questionnaire

Name---------- Date---------- Class----------

1. What does the word bullying mean to you?

2. What do the words Cyber bullying mean?

3. If you felt that you were being bullied in our school, what would you do?

4. If you felt that you were being bullied outside of school, what would you do?

5. Name two actions you could use from our E-safety rules.

6. If you play games on the internet, do you play with people you don't not know personally?

7. Do you know how to report rude or bullying messages on line?

8. Write either your home address or a telephone number you could call in an emergency?

Think then Click

We ask permission before using the Internet.

We only use websites our teacher has chosen.

We immediately close any webpage we don't like.

We only e-mail people our teacher has approved.

We send e-mails that are polite and friendly.

We never give out a home address or phone number.

We never arrange to meet anyone we don't know.

We never open e-mails sent by anyone we don't know.

We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.

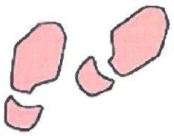
These rules help us to stay safe on the Internet

Think then Click

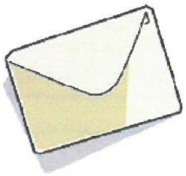
We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.



We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.