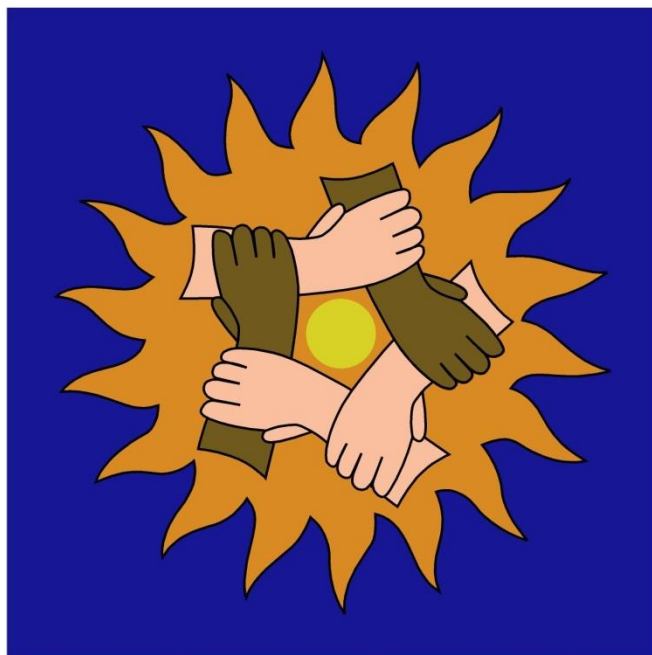# Highfield Primary School

E-Safety Policy and Acceptable Use of ICT Agreements 2016

1. Introduction

At Highfield 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.

Highfield 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 has been contributed to by the whole school and ratified by the governors.

For expectations regarding the taking, distribution and publication of photography and videos at Highfield see the photography and video policy dated January 2016.

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, Photography and Video Policy, and Equal Opportunities Policy.

Introduction of E-Safety Policy and whole school community involved including parents.

Whole school E-Safety training took place September 2015

2. Roles and Responsibilities

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

Maria Kemal (Headteacher) has overall responsibility. Michelle Lynch and Gina Christodoulou (Learning Mentors) 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 e-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 e-safety.
- 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.

Our internet access is controlled through the London Grid for Learning (LGFL) web filtering service.

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. <u>Security and Data Protection</u>

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. <u>E-Safety Complaints/Incidents</u>

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. <u>Review of Policy</u>

There are on-going opportunities for staff, children and families to discuss e-safety concerns with our Learning Mentors. 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.

<u>Appendix</u>

1. Pupil Acceptable Use of Technology Policy 2015 + Infant Consent Form
2. Staff, Governor and Visitor Acceptable Use Agreement
3. Flow chart for managing an e-safety incident not involving any illegal activity
4. Flow chart for managing an e-safety incident involving illegal activity
5. E-Safety Incident Log
6. Advice for children on Cyber bullying – Enfield document
7. Advice for parents on Cyber bullying – Enfield document
8. KS1 Internet tips
9. KS2 Internet tips
10. E-safety questionnaires

Highfield Primary School

Pupil Acceptable Use of Technology Policy
2015

This policy details the expectations regarding pupil's use of technology at Highfield Primary School. The policy covers expectations for all pupils of the school and contains three strands. This policy is to be adhered to during all school activities on and off the school site.

1. Safety

The main purpose of the policy is in regards to safeguarding and to ensure the safety of all pupils and the wider community of the school.

2. Privacy

We welcome and value each member of Highfield's community to their right to privacy and as such each member of the community is entitled to choose not to feature in photographs or videos recorded at the school, on and off site.

3. Protecting Highfield's Image

Use of technology at Highfield should not do anything which may cause any embarrassment to the school, the children, parents, carers, staff, visitors or members of the wider school community.

Changes to permissions

Any failure to adhere to this policy may lead to a withdrawal of permission to use certain technologies at the school for a set period of time.

Pupil Acceptable Use Policy

All pupils must follow the expectations set out in this policy when using technology during all school activities on and off the school site.

Pupils that do not follow these expectations may lead to:

• A withdrawal of permission to use certain technologies at the school for a set period of time.

• A change in the conditions of permission to use certain technologies at the school.

Staff at Highfield will teach pupils the expectations of technology use.

Technology refers to computers, laptops, ipads, tablets, visualisers, photocopiers, cameras, scanners, telephones, mobiles, screens, software, hardware, accessories, internet, social media and any other technology equipment.
Technology Expectations

1. I will use polite language when using the computers.

2. I must not write anything that might: upset someone or give the school a bad name.

3. I know that staff will regularly check what I have done on the school computers.

4. I know that if a member of staff thinks I may have been breaking the rules they will check my prior technology use.

5. I must not tell anyone my name, where I live, my telephone number or other personal information whilst using technology.

6. I must not tell my username and passwords to anyone but my parents.

7. I must never use other people's usernames and passwords or computers left logged in.

8. If I think someone knows my password then I will tell a member of staff.

9. I must ensure technology is switched off/logged off when finished.

10. I know that my technology use is not guaranteed to be private.

11. I must not use the technology in any way that stops other people using it.

12. I will report anything that makes me feel uncomfortable to a member of staff.

13. I will tell a member of staff straight away if I am sent messages that make me feel uncomfortable.

14. I will not damage any technology equipment or the work of another person.

15. If I see something I am uncomfortable with or is inappropriate I must tell a member of staff straight away and not share it with other pupils.

Unacceptable Use of technology

Examples of unacceptable use include, but are not limited to:

1. Using another person's username and password.
2. Creating or sending messages/pictures of other content that might upset other people.
3. Changing/editing/deleting work that belongs to other people without permission. Waste time or resources using school technology.
4. Misusing or damaging technology.
5. Using technology without permission from member of staff and continuing to use after being asked to stop.
6. Sending, sharing personal information.

Infant Consent Form

Child's Name _____ Class _____

Admission Date _____

I will discuss the school booklet with my child and I will support the Home School Agreement.   Yes   No

Outings, Trips and Off Site Activities

Staff at Highfield will always inform you of trips and school journeys and require you to fill out consent forms for journeys incorporating coaches, trains, etc. However, for smaller off site activities and local visits please give your permission here.

I understand that on occasions whilst at Highfield my child will be taken off the premises to visit shops, libraries, parks or other places of interest. At such time I understand that there will be at least one adult, in a small group, or three or four accompanying a class. I give permission for my child to be taken out of school on these visits.
Yes   No

ICT

I have read the Pupil Acceptable Use of Technology Policy (in school booklet) with my child and agree to the expectations set out.
Yes   No

I understand that if my child does not follow the expectations it will mean they may have their use stopped, more closely monitored or past use investigated.
Yes   No

Photographic permission

I give permission for my child's photograph to be taken if necessary and used within the context of the school, including the school website.
Yes   No

I give permission for my child to be included in any video footage used within the context of the school. This may be uploaded on to the school website.
Yes   No

I give permission for my child's photograph to be used in other publications, such as the local Newspaper.
Yes   No

Food Tasting and Allergies

I give permission for my child to take part in food tasting.
Yes   No

My child cannot eat _____

My child has the following allergies _____

Parent/Carer Signature _____ Date _____ 7

Highfield Primary School

<center><u>Appendix 2</u></center>

<center><u>Highfield Primary School</u>
<u>Acceptable Use of ICT Agreement</u></center>

<center># Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct</center>

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 Maria Kemal, Headteacher or a member of the CP 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 Scholar Pack) 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 will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.**

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

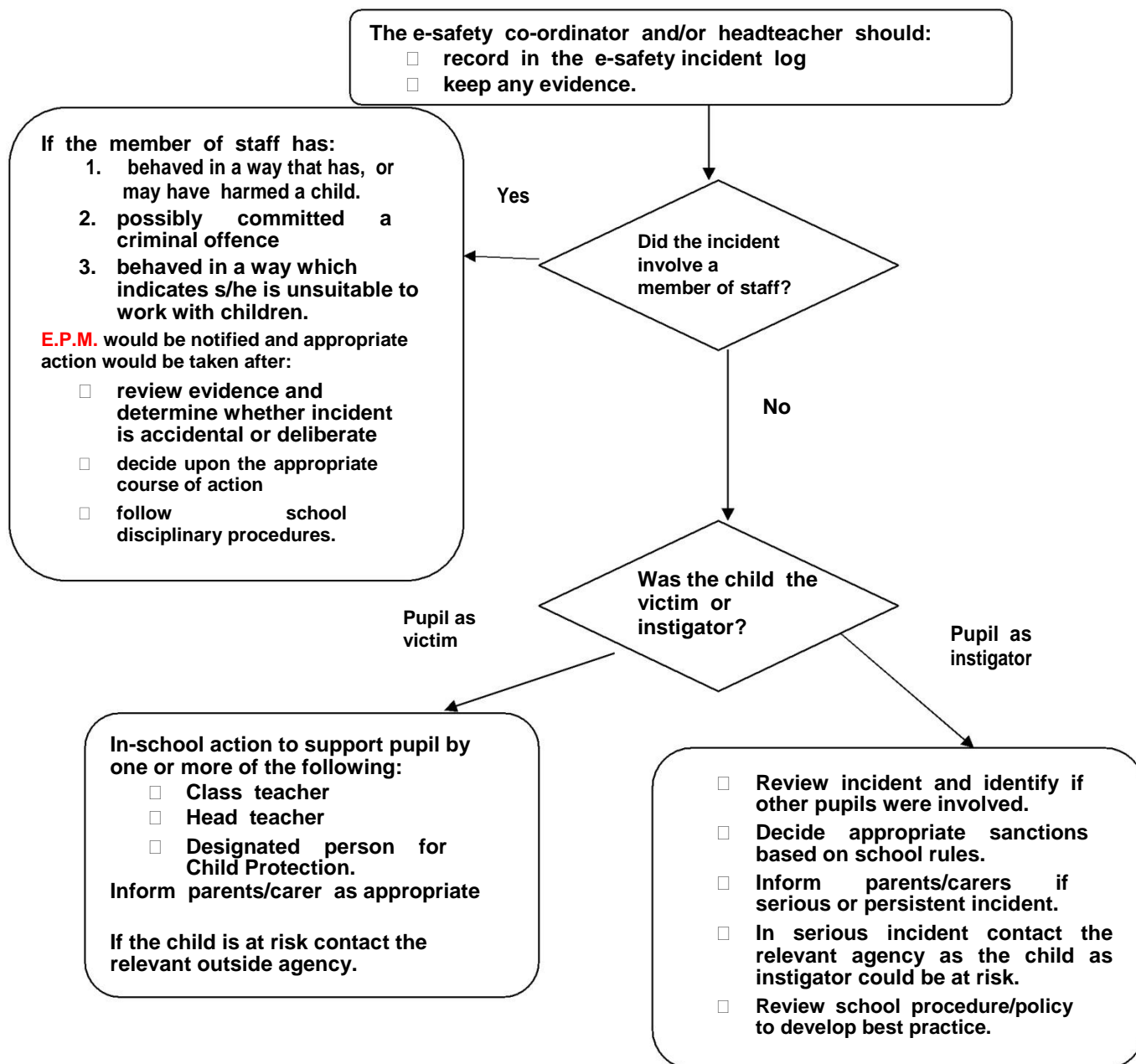**Signature …………………….………… Date ……………………**

Full Name …………………………………..................................... (printed)

Job title: ………………………………………………………………..

Appendix 3

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

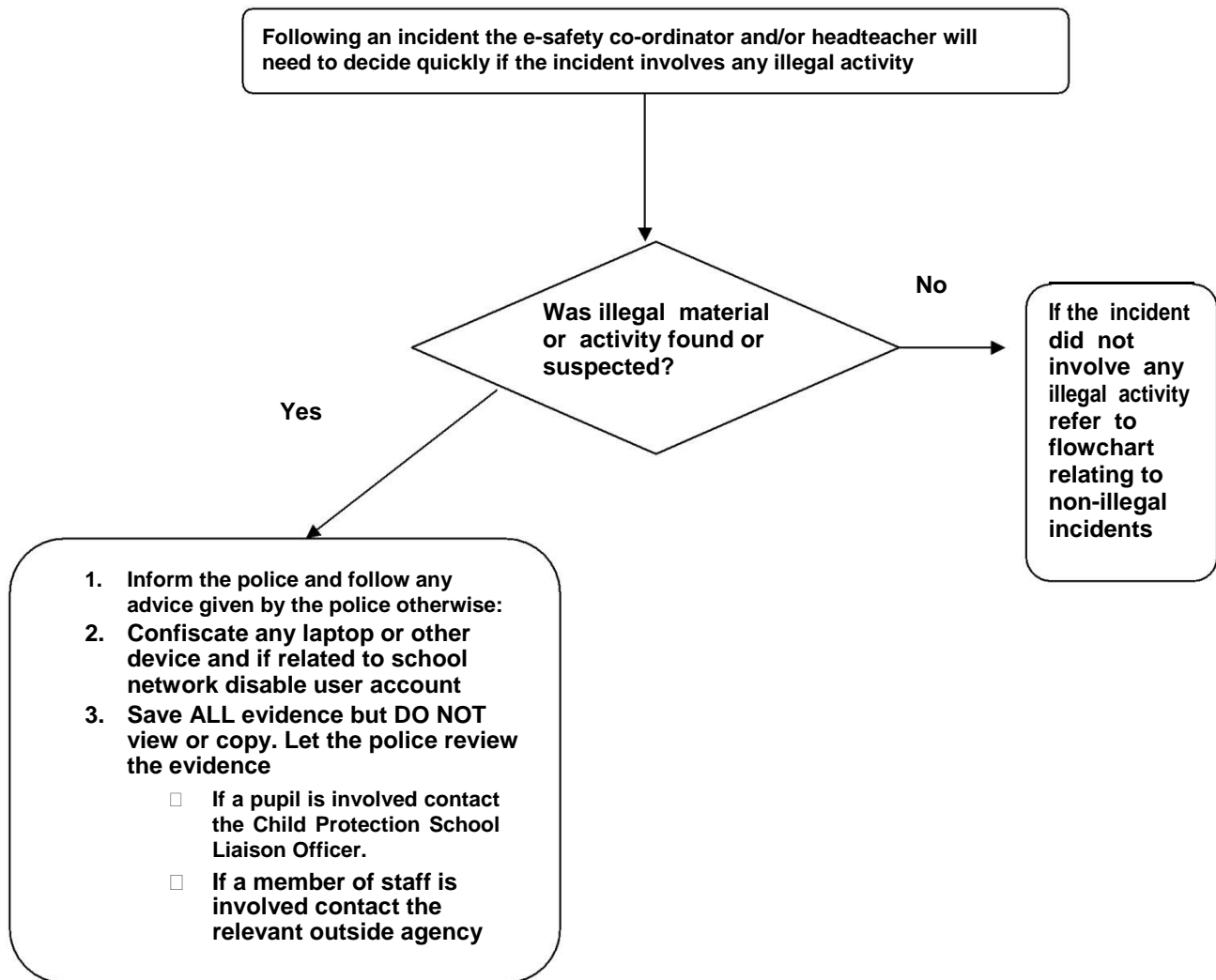**Incidents not involving any illegal activity, such as:**
- ☐ **using another person's user name and password**
- ☐ **accessing websites which are against school policy**
- ☐ **using a mobile phone to take video during a lesson**
- ☐ using the technology to upset or bully (in extreme cases this could be illegal)

The e-safety co-ordinator and/or headteacher should:
- ☐ **record in the e-safety incident log**
- ☐ **keep any evidence.**

Did the incident involve a member of staff?

Yes

If the member of staff has:
1. behaved in a way that has, or may have harmed a child.
2. possibly committed a criminal offence
3. behaved in a way which indicates s/he is unsuitable to work with children.

E.P.M. would be notified and appropriate action would be taken after:
- ☐ review evidence and determine whether incident is accidental or deliberate
- ☐ decide upon the appropriate course of action
- ☐ follow school disciplinary procedures.

No

Was the child the victim or instigator?

Pupil as victim

Pupil as instigator

In-school action to support pupil by one or more of the following:
- ☐ **Class teacher**
- ☐ **Head teacher**
- ☐ **Designated person for Child Protection.**

Inform parents/carer as appropriate

If the child is at risk contact the relevant outside agency.

- ☐ **Review incident and identify if other pupils were involved.**
- ☐ **Decide appropriate sanctions based on school rules.**
- ☐ **Inform parents/carers if serious or persistent incident.**
- ☐ **In serious incident contact the relevant agency as the child as instigator could be at risk.**
- ☐ **Review school procedure/policy to develop best practice.**

E-Safety Policy February 2016

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**

> **Following an incident the e-safety co-ordinator and/or headteacher will need to decide quickly if the incident involves any illegal activity**

Was illegal material or activity found or suspected?

No

Yes

If the incident did not involve any illegal activity refer to flowchart relating to non-illegal incidents

1. **Inform the police and follow any advice given by the police otherwise:**
2. **Confiscate any laptop or other device and if related to school network disable user account**
3. **Save ALL evidence but DO NOT view or copy. Let the police review the evidence**
   - **If a pupil is involved contact the Child Protection School Liaison Officer.**
   - **If a member of staff is involved contact the relevant outside agency**

Highfield Primary School E-Safety Incident Log

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

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

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.

Highfield Primary School

- ☐ 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

- ☐ Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.
- ☐ If someone insults you online or by phone, stay calm – and ignore them.
- ☐ 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.

Advice for Parents and Children on Cyber-bullying

Key Safety Advice

The whole school community has a part to play in ensuring cyber safety. Understanding children and young people's online lives and activities can help adults respond to situations appropriately and effectively. Asking children and young people to show adults how technologies and services work is a useful strategy that can provide an important learning opportunity and context for discussing online safety.

For children and young people

1: Always respect others – be careful what you say online and what images you send.
2: Think before you send – whatever you send can be made public very quickly and could stay online forever.
3: Treat your password like your toothbrush – keep it to yourself. Only give your mobile number or personal website address to trusted friends.
4: Block the bully – learn how to block or report someone who is behaving badly.
5: Don't retaliate or reply!
6: Save the evidence – learn how to keep records of offending messages, pictures or online conversations.
7: Make sure you tell:
  - an adult you trust, or call a helpline like ChildLine on 0800 1111 in confidence;
  - the provider of the service; check the service provider's website to see where to report incidents;
  - your school – your teacher or the anti-bullying coordinator can help you.

Finally, don't just stand there – if you see cyberbullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?

For parents and carers

1: Be aware, your child may as likely cyberbully as be a target of cyberbullying. Be alert to your child seeming upset after using the internet or their mobile phone. This might involve subtle comments or changes in relationships with friends. They might be unwilling to talk or be secretive about their online activities and mobile phone use.
2: Talk with your children and understand the ways in which they are using the internet and their mobile phone. See the seven key messages for children (on the left) to get you started.
3: Use the tools on the service and turn on in-built internet safety features.
4: Remind your child not to retaliate.
5: Keep the evidence of offending emails, text messages or online conversations.
6: Report cyberbullying:
  - Contact your child's school if it involves another pupil, so that they can take appropriate action.
  - Contact the service provider.
  - If the cyberbullying is serious and a potential criminal offence has been committed, you should consider contacting the police.

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.

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.

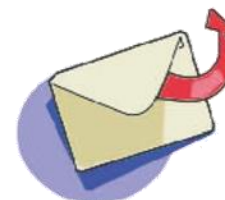We only e-mail people our teacher has approved.

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.

Kent Community Network

J. Barrett & H. Barton

Kent County Council

<div align="center">

<u>Anti-Bullying & Cyber bullying questionnaire KS1</u>

<u>Autumn Term 2015</u>

</div>

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 Highfield 5? …..………...............**

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

Autumn Term 2015

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 'The Highfield Five'.

     _____

6. What is the 'Red Box' in our school used for?

     _____

7. What do the Mini Mentors do in our school? Where can you find them?

     _____

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

     _____

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

     _____

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

     _____