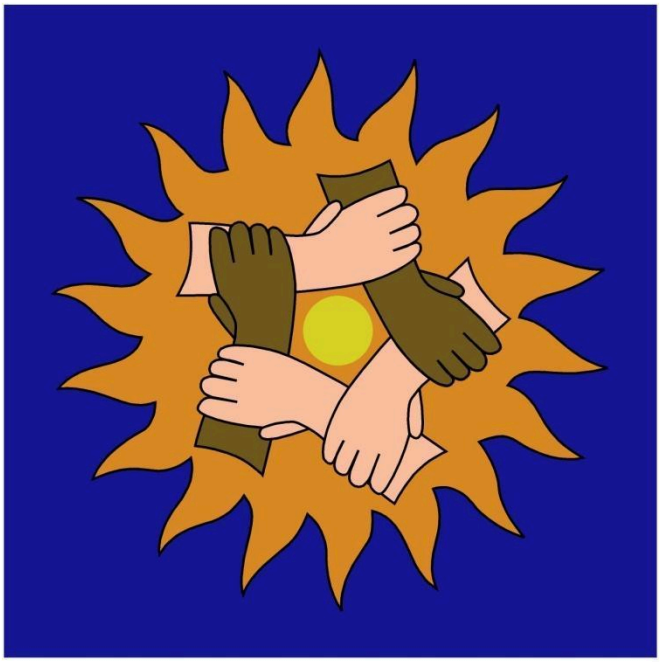
"Together we can achieve more"

Highfield Primary School



E-Safety Policy and Acceptable Use of technology Policy

2024

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 takes place as part of our annual KCSIE training.

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.

David Wilson (Headteacher) has overall responsibility although children can report to any member of staff if they have concerns.

It is the role of the school's child protection team 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 (including social media)
- 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. <u>Curriculum</u>

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.
- 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 child protection team 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 our child protection team. 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. Pupil Acceptable Use of Technology Policy
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

Highfield Primary School

Appendix 1

Pupil Acceptable Use of Technology Policy
2024

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.

Highfield Primary School

Appendix 2

Highfield 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 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

Parent/Carer Signature _____

Signature ……. Date ……

Full Name ……..... (printed)

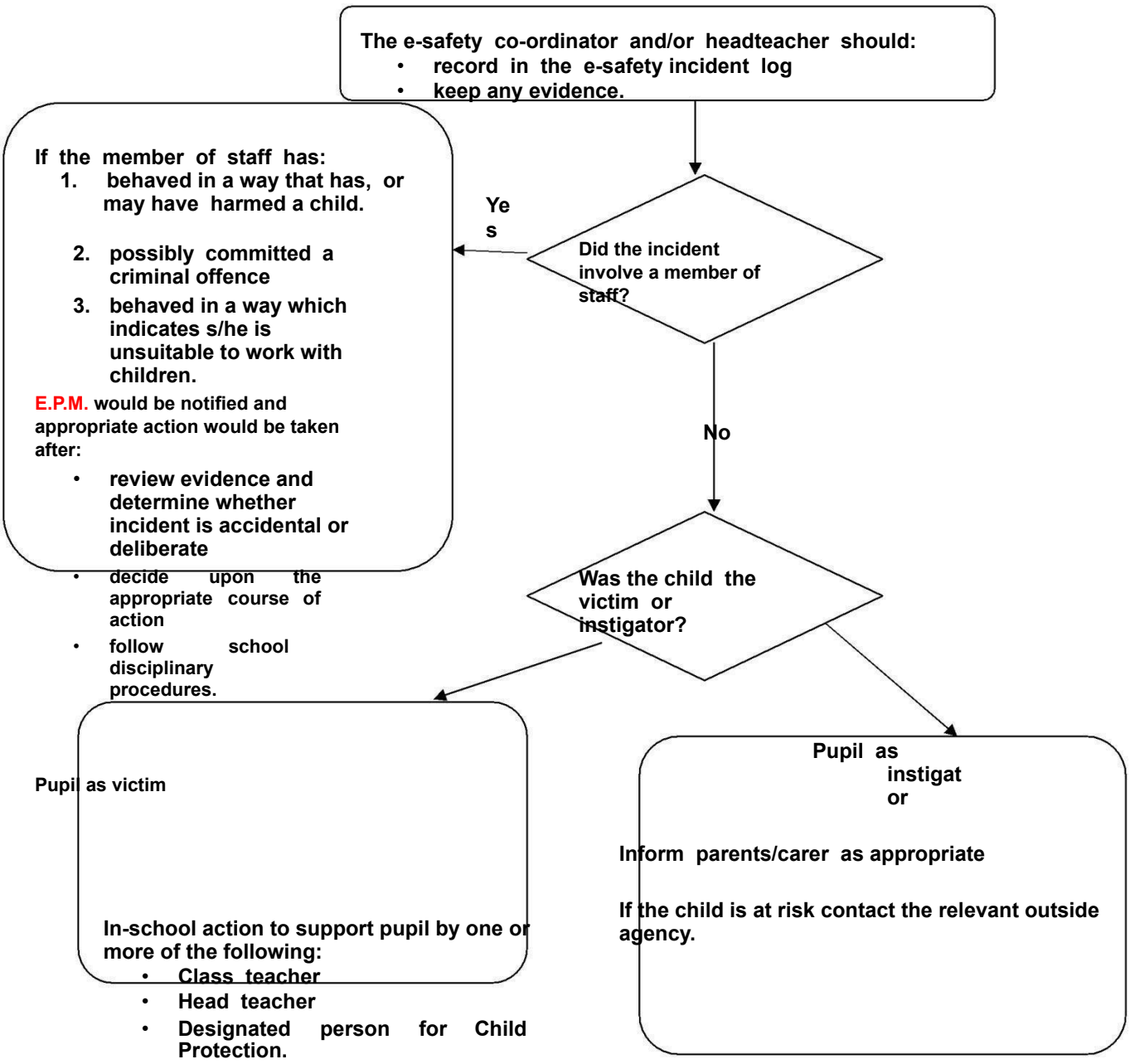
Job title: ……..

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)**



- **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.

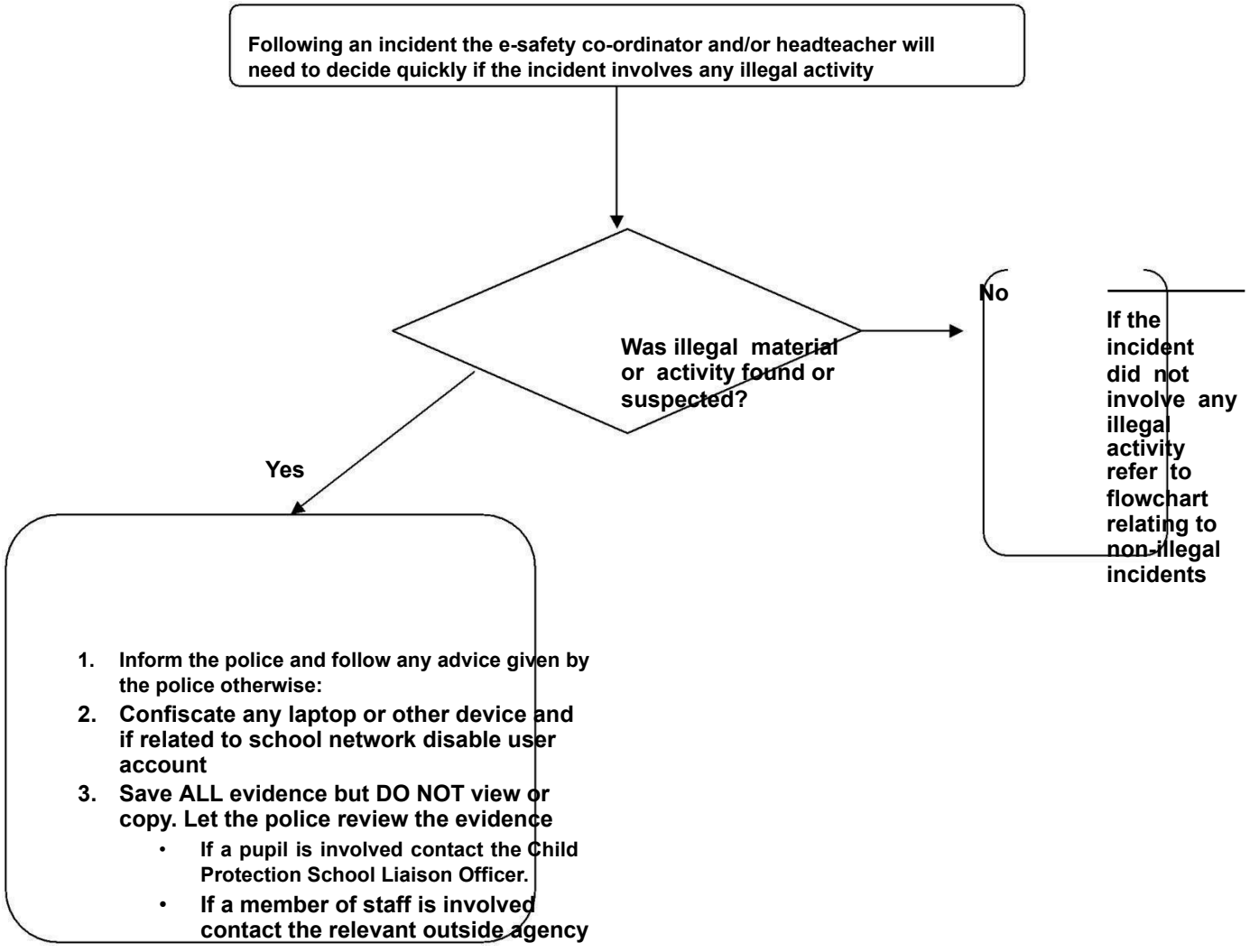
Review school procedure/policy to develop best practice.

Appendix 4

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 5

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

Appendix 6

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.

- 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

Please check our useful links regarding keeping your child safe on line and how to implement parental controls on devices please go to our online safety page on the school's website. https://www.highfieldprimary.co.uk/health-wellbeing/online-safety/

Next Review date Nov 22