Online Safety Policy

Date: September 18

Person responsible:	**B Huitson**
Date ratified:	**October 18**
Chair of Governors:	**I Trevitt**
Head teacher:	**S Nordstrom**
Date of review:	**September 2019**

Introduction – include the school's vision for IT here:

At Easington Lane Primary, our IT vision involves and includes the whole school community including: current and former pupils; parents; staff; outside agencies; governors; our cluster of schools and the local community. Our aspirations are to use IT to support high standards of achievement. We believe that effective use of IT enables our pupils to develop the confidence to apply their learning and skills to overcome challenges and reach their full potential. We believe that IT is a powerful tool to help raise pupils' expectations, offering new opportunities and experiences. We will harness the power of technology to encourage creativity, encouraging full participation in learning activities. We believe that innovative use of technology supports independent and flexible learning. We aspire to provide opportunities for pupils to become experts and to share their IT knowledge with other pupils and adults. We want to promote IT as a tool to enable learning both at home and in school.

Our vision includes promoting respectful behaviours with and through technology. We are committed to providing IT learning opportunities which are well managed and which deliver high standards of Online Safety, effectively managing risk of harm to learners. We want all learners to become responsible for their own actions and safety when working with technology.

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Media
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Cloud Based Learning Environments
- Other mobile applications with web functionality

'Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks'
Becta Safeguarding Children Online Feb 2009

Whole School Approach to the safe use of IT

Creating a safe IT learning environment includes three main elements:

- Appropriate digital technology which is well managed to protect users, data and systems
- Acceptable Use Policies (AUPs) and procedures, with clear roles, responsibilities and sanctions for deliberate infringement of acceptable use

- A comprehensive E-Safety education programme for pupils, staff and parents which meets the requirements of the National Curriculum.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership and the Head Teacher is personally responsible for the safety of users, data and systems. The Governing Body aims to support the Head Teacher embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and has ultimate responsibility to ensure that the policy and practices are applied, monitored and reviewed.

The named E-Safety co-ordinators in our school are: S Nordstrom, B Huitson and S Johnson

AUPS –(Acceptable Use Policy) (Appendix 2)

- All staff are required to sign the AUP each year. A record will be kept in the school office. All users, including non-teaching staff, visitors and helpers must read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety rules.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

Managing the school E-Safety messages

- The school embed E-Safety messages across the curriculum to meet the requirements of the National Curriculum.
- E-Safety messages will be prominently displayed in classrooms and public areas.
- The school will work with the Governing Body to provide a range of information, support and advice to parents and carers on how to keep their children safe when online at home.

E-Safety and the National Curriculum

IT and online resources are increasingly used across the curriculum. The school will ensure that it meets its statutory requirements for teaching E-Safety. The school will look continually for new opportunities to promote E-Safety messages with the school community.

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, business and social interaction, as well as a potential risk to young and vulnerable people. Within school:

- Internet access within the school is filtered in line with national recommendations
- Internet usage is monitored and inappropriate use is logged
- 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
- The school will only use Google Safe Search when searching for images

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. Parents will be advised to recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to an E-Safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines. The network manager is responsible for: ensuring that all machines are logged onto the school domain; that all sensitive data is backed up safely and all machines and storage devices which are taken offsite are encrypted using up to date, robust systems.

Access to Technology

- Each child is provided with a user area which means they will have a secure password protected area on the school network and when using the internet.
- Pupils will be taught that their password must be kept confidential.
- Pupils will be taught that if they think their account has been compromised then they must report it to a member of their teaching staff.
- Pupils will be taught how to use their e-mail account responsibly. The school takes allegations of internet misuse including online bullying very seriously.

E-mail

The use of email within school is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or externally. The school recognises that pupils need to understand how to style an email in relation to their age. By the end of Key Stage 2, pupils must have experienced sending and receiving emails.

- Pupils are introduced to email as part of the IT Scheme of Work.
- The school gives staff and governors their own email account. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff must not use their personal email in relation to any school business.
- Pupils may only use school approved accounts on the school system.
- The forwarding of chain letters is not permitted in school.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Everyone must use appropriate language in e-mails, must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff must inform an E-Safety co-ordinator if they receive an offensive e-mail.

Publishing pupil’s images and work

On a child’s entry to the school, all parents/guardians will be asked to give permission for their child’s photo to be taken and to use their child's work/photos in the following ways:

- on the school web site

- on Earwig (online learning journey)
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Images must only be stored on the school server and images of pupils who have left the school should be deleted. Pupils' names will not be published alongside their image and vice versa without permission from the parents. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published if work is published on the internet.

Social networking and personal publishing

We filter access for pupils to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Pupils will be advised never to give out personal details of any kind which may identify them or their location. Where the school uses social media to communicate with the school community, the school will monitor and manage all activity very closely.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- All pupils are supervised by a member of staff when video conferencing
- Approval from the Head teacher is sought prior to all video conferences within school.

Use of Personal Mobile Devices

Personal devices are very common however there are clear guidelines as to when and how they should be used when in the school environment.

- Staff are only permitted to use their mobile devices in 'Mobile Safe Zones' (indicated by signage) during the school day. ~
- Although breakfast and tea time clubs run outside of the school day, these are held at the extremities of the building and therefore mobile device usage is permitted in classrooms (not corridors).
- Regardless of the above points, mobile devices should not be used whenever a child is present/visible.

Pupils should not be in school with a mobile device. In the event of a child bringing a device to school it should be brought to the main school office when it will be secured safely until the end of the school day.

More information about the management of these procedures can be found in the Appendix Section - *Flowchart for Managing an E-Safety incident*

~for the purposes of this policy the school day means 08:55 to 16:00 to include after school clubs

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Password and System Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Passwords will be changed on a regular basis, at least twice a year or more frequently. Pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- If a password may have been compromised or someone else has become aware of the password, the child or adult must report this to an E-Safety co-ordinator
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, accounts, including ensuring that passwords are not shared and are changed periodically.
- All users must log on and log off after a session. **Individual staff users must also make sure that workstations are locked automatically if left unattended**.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Data can only be accessed and used on school computers or laptops. Data taken off site will be on encrypted hardware. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data unless effective authentication provides authorised access.

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.legislation.gov.uk/ukpga/1998/29/contents

Responding to E-Safety incidents/complaints

The school will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

- Concerns relating to E-Safety should be made to an E-Safety co-ordinator. Any complaint about staff misuse must be referred to the Head teacher. Incidents should be logged and the Flowcharts for Managing an E-Safety Incident should be followed (see Appendix 3).

- All users are aware of the procedures for reporting accidental access to inappropriate materials.
- The breach must be immediately reported to the school's E-Safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged. Depending on the seriousness of the offence; investigation may involve the Head teacher and/or the LA. This may lead to disciplinary or legal action. (Appendix 4)
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Online bullying

Online bullying is the use of IT, particularly mobile phones and the internet, deliberately to upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site'. Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of online-bullying. Here are some of the more common:
1. **Text messages** —that are threatening or cause discomfort - the sending of anonymous text messages over short distances using "Bluetooth" wireless technology
2. **Picture/video-clips** via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
3. **Mobile phone calls** — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
4. **Emails** — threatening or bullying emails, often sent using a pseudonym or somebody else's name.
5. **Chatroom bullying** — menacing or upsetting responses to children or young people when they are in web-based chatroom.
6. **Instant messaging** (IM) — unpleasant messages sent while children conduct real-time conversations online
7. **Bullying via websites and social media** — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites.
The best way to deal with online bullying is to prevent it happening in the first place and to have clear steps to take when responding to it.
8. **Typing abusive comments** via a word processor or other package and then deleting the message before it is seen by an adult.

Preventing online bullying

It is important that we work in partnership with pupils and parents to educate them about online bullying as part of our E-Safety curriculum.
They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are bullied online

- report any problems with online bullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP).

Communications Policy

Introducing the E-Safety policy to pupils

- E-Safety rules will be posted in all classrooms and discussed with pupils (see appendices for E-Safety posters for KS1 and KS2.)
- Pupils will be informed that network and Internet use will be monitored.

Introducing staff to the E-Safety policy

- All staff will be given the E-Safety policy and its application and importance will be explained. All staff will sign the AUP annually.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on our E-Safety policy will be provided as required.

Enlisting parents' support – (Appendix 1)

The school believes that it is essential for parents/ carers to be fully involved with promoting E-Safety both in and outside of school. The school will regularly consult and discuss E-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to IT.

The school disseminates information to parents relating to E-Safety where appropriate in the form of:

- Information events and assemblies
- Posters
- Website postings
- Newsletter items
- Parents/carers are asked to read and sign the school's AUP alongside their child's signature. This will be done annually.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- A partnership approach with parents will be encouraged. This includes parents' evenings with suggestions for safe home Internet use.
- Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

Reviewing this Policy

This policy will be reviewed, along with the Acceptable Use Policy, on a yearly basis. It will encompass new technologies and developments. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way. Staff, governors, parents and children will be consulted on any changes.

Appendix 1

SECTION 3 – ONLINE SAFETY RULES AND AGREEMENT OF USE

The school believes that technology plays a significant role right across the curriculum. The school promotes safe and acceptable use of technology including, email, the internet and social media. The below rules indicate the school's expectation of pupils when accessing technology.

- ✓ I will use IT only in school for school purposes.
- ✓ I will use only my class e-mail address or my own school e-mail address when e-mailing.
- ✓ I will open only e-mail attachments from people I know, or whom my teacher has approved.
- ✓ I will not tell other people my passwords.
- ✓ I will only open/delete my own files.
- ✓ I will not bring software, CDs or IT equipment into school without permission.
- ✓ I will only use the Internet after being given permission from a teacher.
- ✓ I will make sure that all online contact with other children and adults is responsible, polite and appropriate.
- ✓ I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I find anything like this accidentally, I will minimise 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 arrange to meet someone.
- ✓ I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- ✓ I know that the school may check my use of technology 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 E-Safety.

Parent's/Carer's Consent for Internet Access

I have read and understood the school's Acceptable Use Policy for IT and give permission for my son / daughter to access the Internet and other technologies in school. I understand that the school will take all reasonable precautions to keep pupils safe and to prevent access to inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I agree that should my son/daughter need to access the internet at home or anywhere else, that I will take all reasonable precautions to ensure he/she cannot access inappropriate materials and that he/she will use the computer in an appropriate manner.

Signed_____________________________________ (Parent/carer) Date_________________

EARWIG

The school uses a software package called Earwig to help track your child's Learning Journey from the start till the end of school. The Earwig system is secure and can be used to upload photos and videos that celebrate your child's journey. As a parent you will also receive a bespoke password to track and monitor your child's progress.

Please tick and sign the below;

□ I give permission for my child's images, videos or audios to be uploaded securely onto Earwig

□ I do not give permission for my child's images, videos or audios to be uploaded securely onto Earwig

My email address is ____

Signed: ____ Date: _________________

Appendix 2

Acceptable User Agreement

Staff, Governor and Authorised Visitor

IT and related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This Agreement is designed to ensure that all personnel are aware of their professional responsibilities when using any form of IT. All personnel operating in school are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher. I understand that I will be required to sign this agreement each year.

Code of Conduct

Laptops, Computers and Mobile Devices

- I will only use the school's equipment, email / Internet/ Cloud Technologies and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will only use my personal mobile device in designated **Mobile Safe Zones** or in a safe place outside of the school day. I will not use my device in the presence of pupils. If utilising the school's wi-fi connection using a personal device the above point remains applicable.

Information Security

- If I am provided with a school device I will ensure that the device has a password on it in the event it is lost or stolen.
- I will change my password as required for all logins.
- I will log off/ lock my computer when it is not in use.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will only use the school's approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. I understand that I am responsible for safeguarding data or systems if I am allowed to take these offsite. No sensitive data relating to pupils or staff will be stored on my local machine when off site.
- I understand that any laptop or mobile device off site is school property and will not be used by non-employees including family.
- I know that staff or pupil 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 or software without permission from the E-Safety co-ordinators or ICT corporate partners.
- I understand that images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school Photography and Digital Imagery 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 I must not use my own equipment to take images of pupils. I understand that any images taken using official school equipment must be transferred to the school server and then deleted from the original device.
- I understand that the use of USB sticks, external hard drives and device used to extract and store data are strictly forbidden without prior agreement from the E-Safety coordinator.
- I understand that all camera memory cards must be logged as an electronic asset via the School Business Manager.

Internet Access, Social Media & Communication

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that all my use of the Internet and other related technologies will be monitored and logged and can be made available, on request to 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 or the school into disrepute.
- 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 support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of IT and related technologies.
- I will ensure that only children whose parents have given permission for them to use the Internet and IT are enabled to do so at school.
- Any authorised visitor wanting to use technology for teaching purposes must email resources to the relevant staff prior to use.

User Signature

By signing the this document, I acknowledge that this agreement complies with the requirements set out in Keeping Children Safe in Education and the General Data Protection Regulations. I agree to comply with this Agreement and understand that failure to do so could lead to disciplinary action.

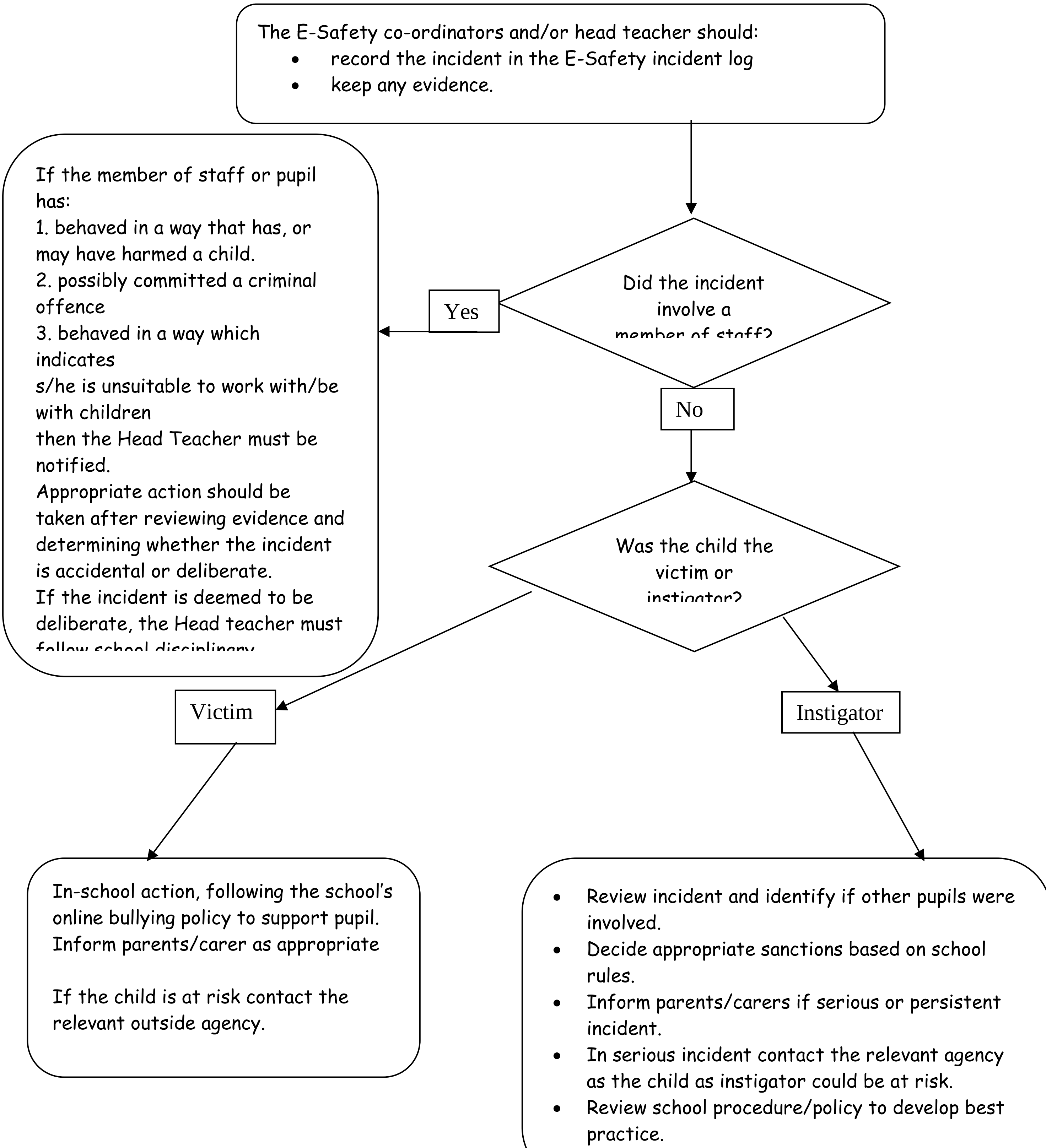
Signature ……………………………… Full Name ……………………………… (Printed)
Date………………………

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 during lessons or in prohibited places
- using the technology to upset or bully (in extreme cases this could be illegal.)



The E-Safety co-ordinators and/or head teacher should:

- record the incident in the E-Safety incident log
- keep any evidence.

Did the incident involve a member of staff?

Yes

If the member of staff or pupil 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/be with children
then the Head Teacher must be notified.
Appropriate action should be taken after reviewing evidence and determining whether the incident is accidental or deliberate.
If the incident is deemed to be deliberate, the Head teacher must follow school disciplinary

No

Was the child the victim or instigator?

Victim

In-school action, following the school's online bullying policy to support pupil.
Inform parents/carer as appropriate

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

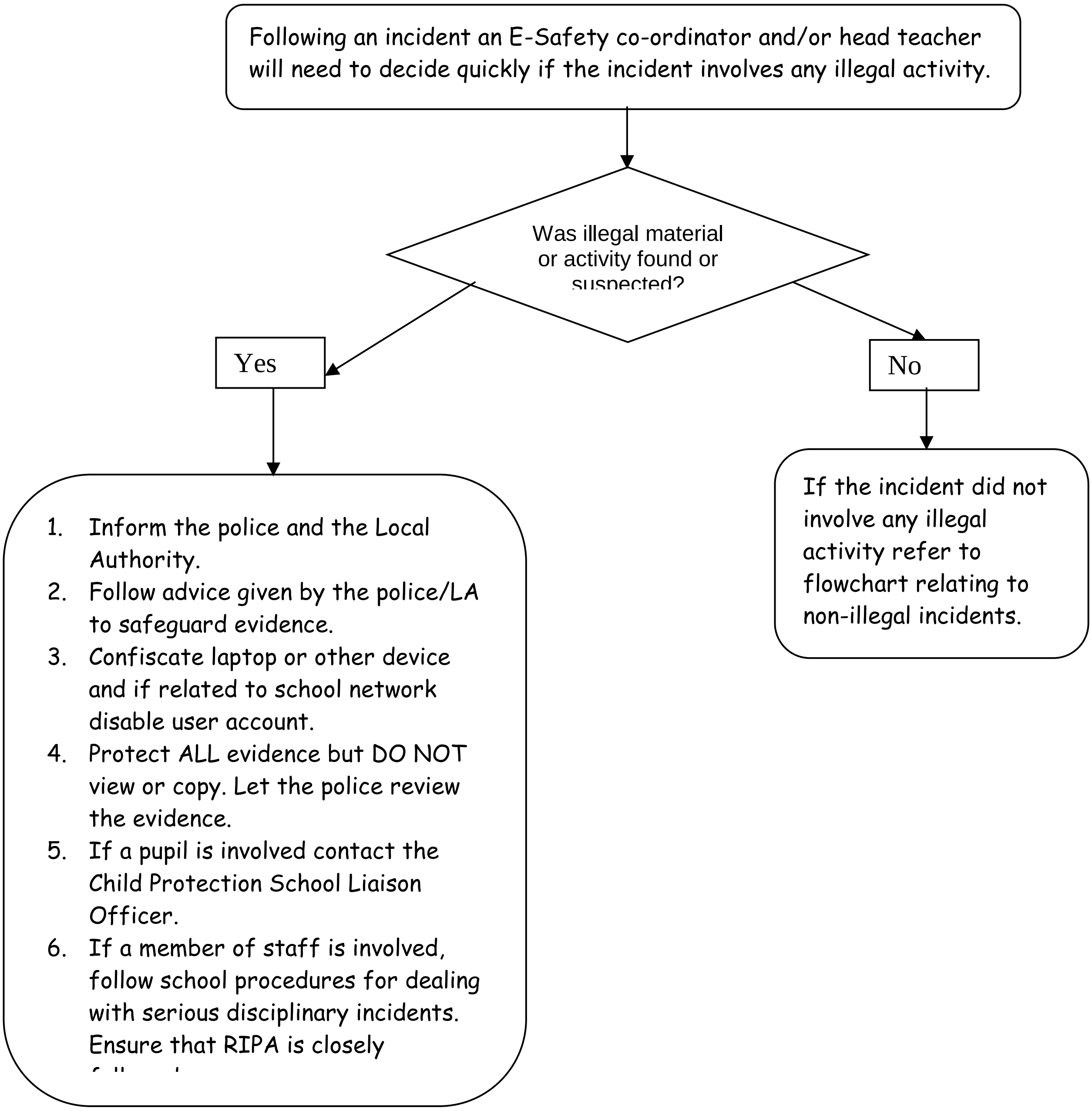
Instigator

- 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.

Flowchart for Managing an E-Safety incident involving illegal activity

Illegal means something against the law, such as:

- accessing images of child abuse
- duplicating or passing on images or video containing child abuse
- inciting racial or religious hatred
- promoting illegal acts



Following an incident an E-Safety co-ordinator and/or head teacher will need to decide quickly if the incident involves any illegal activity.

Was illegal material or activity found or suspected?

Yes

1. Inform the police and the Local Authority.
2. Follow advice given by the police/LA to safeguard evidence.
3. Confiscate laptop or other device and if related to school network disable user account.
4. Protect ALL evidence but DO NOT view or copy. Let the police review the evidence.
5. If a pupil is involved contact the Child Protection School Liaison Officer.
6. If a member of staff is involved, follow school procedures for dealing with serious disciplinary incidents. Ensure that RIPA is closely followed.

No

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

Appendix 4

E-Safety Incident Log

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

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