E-Safety Policy

Langenhoe Community Primary School

PREPARED BY:

Alice Badman
Computing Leader for Learning
E-safety Officer

APPROVED BY:

Governing Body

ISSUE AND REVISION RECORD

Date	Details	Review date
Oct 04	Internet Safety Policy	Oct 06
Oct 06	Internet Safety Policy	Oct 09
Oct 09	Revised	Oct 10
Oct 10	Change name pg 3	Oct 11
Oct 11	E-folio changed to Web Any Where	Oct 12
Oct 12	Revised	Oct 13
Mar 14	Revised	Mar 15
Mar 15	Revised – Purple Mash	May 16
May 16	Revised – cyber bulling and radicalisation	May 17
May 17	Removal of Web Anywhere	May 18

Langenhoe Community Primary School
E-Safety Policy

1. Introduction

Computing in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing within the curriculum is broken down into three areas; Computer Science, Information Technology and Digital Literacy.

Digital Literacy is regarded as allowing children *'to use and express themselves safety in a digital world' (e-safety).*

E-Safety covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of technology within our society as a whole. Currently the technology children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, photo, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much technology, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Langenhoe Community Primary School**,** we understand the responsibility to educate our pupils on e-safety issues; teaching them the 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.

'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 Information Technology

Creating a safe learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-safety education programme for pupils, staff and parents

2. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head teacher, with the support of the Governors, aims to 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 embedded and monitored.

The named E-Safety Officer in our school from September 2013 is Alice Badman.

All members of the school community have been made aware of who holds this post. It is the role of the E-safety Officer to keep abreast of current issues and guidance through organisations such as Essex LEA, CEOP (Child Exploitation and Online Protection) and Child net.

The E-safety Officer ensures the Headteacher, 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.

After every review all staff should be familiar with the schools' policy including:

- Safe use of e-mail
- Safe use of the Internet
- Safe use of Purplemash
- 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 appendix 5 & 6)
- Their role in providing e-safety education for pupils
- Steps to take should they be concerned about a child
- The use of social networking

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 (see appendix 1 for staff acceptable use agreement).

Governors are reminded/updated about e-safety and new governors receive information on the Governor's acceptable use policy (see appendix 2 for Governor's 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. E-safety in the curriculum

Technology 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 opportunities to promote e-safety.

- We are implementing a framework for teaching internet skills within the IPC Curriculum, E-Safety lessons and Circle Time.
- 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 E-Safety lessons.
- Pupils are aware of the impact of online bullying through E-Safety Lessons 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 **(see section 8. Cyber bullying)**
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the IPC

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

- We maintain students will have supervised access to Internet resources (where reasonable) 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 this work. Parents will be advised to supervise any further research.
- Our internet access is controlled through Essex LEA's 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 (via hector protector on children's laptops) and the incident reported immediately to the E-Safety Officer.
- 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.

4.1 Purple Mash

Purple Mash is a secure website filled with education resources to support children's learning. Each child uses their own log in to access the website both at home and at school. Staff are able to monitor the children usage.

- Pupils and parents will sign an acceptable use agreement before using the website
- Pupils are taught to keep their password a secret
- If pupils think their account has been compromised then they must report it to their teacher
- The E-safety Officer and ICT technician can monitor individual pupils accounts and pupils access can be filtered or denied

4.2 E-mail

The use of email within most schools 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 international. We recognise that pupils need to understand how to style an email in relation to their age. Children can access their email via Learn Anywhere.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- 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.
- All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff must inform (the e-safety officer) if they receive an offensive e-mail.
- The ICT technician will routinely check children's email accounts for any in proper use.

4.3 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 Purple Mash
- 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)

(See appendix 5)

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting pupils work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Webcams and CCTV

- The only people who have access to the CCTV are the head teacher and office staff.
- We do not use publicly accessible webcams in school.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

4.4 Social networking and personal publishing

We block/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.
- All staff are advised not to use social networking sites on school computers.
- All staff are advised not to allow pupils, past pupils or parents associated with the school to have access to their own personal social network profiles and to adjust their privacy settings accordingly.
- All staff are advised on ways to keep themselves save on social media should they use it.

4.5 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.

4.6 Managing emerging technologies

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

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils or parents are required.

5. Password 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. The 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.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Users are provided with an individual network, email and Purple Mash log-in username. Children are expected to use a personal password to access their Purple Mash account and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the e-safety officer
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

6. 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. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data

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.hmso.gov.uk/acts/acts1998/19980029.htm

7. Responding to e-safety incidents/complaints

As a school we 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. Neither the school nor Essex LEA can accept liability for material accessed, or any consequences of Internet access. Complaints relating to e-safety should be made to the 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 6, 7 & 8).

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety officer.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety officer, depending on the seriousness of the offence; investigation by the Head teacher/ Essex LEA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart in appendix 6 & 7.)
- Pupils and parents will be informed of the complaints procedure
- Parents and pupils will need to work in partnership with staff to resolve issues

8. Cyberbullying

Cyberbullying is the use of technology, 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 cyber-bullying. Here are some of the more common:
1. **Text messages** —that are threatening or cause discomfort - also included here is "bluejacking" (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 using MSN (Microsoft Messenger) or Yahoo Chat
7. **Bullying via websites** — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Facebook and Twitter.

The best way to deal with cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

8.1 Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about cyberbullying 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 being cyberbullied; report any problems with cyberbullying. 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) to do something about it.
- See section 9.3 for more detail

Additional online advice on how to react to cyberbullying can be found on **www.kidscape.org** and **www.wiredsafety.org**

See appendix 8 & 9 for Key Safety Advice for children, parents and carers

8.2 Supporting the person being bullied

- Give reassurance that the person has done the right thing by telling someone and inform parents
- Make sure the person knows not to retaliate or return the message
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
- Take action to contain the incident when content has been circulated
    - Remove content
    - Contact the host (social networking site) to get the content taken down
    - Use disciplinary powers to confiscate phones that are being used to cyberbully – ask the pupil who they have sent messages to
    - In case of illegal content (see appendix managing an e-safety incident involving illegal activity)

8.3 Investigating Incidents

All bullying incidents should be recorded and investigated in the Langenhoe e-safety incident log (see appendix 8).

- Advise pupils and staff to try and keep a record of the bullying as evidence.
- Take steps to identify the bully, including looking at the schools systems, identifying and interviewing possible witnesses, and contacting the service provider and police if necessary. The police will need to be involved to enable the service provider to look into the data of another user.

8.4 Working with the bully and sanctions

- Once the bully is identified, steps should be taken to change their attitude and behaviour by educating them about the effects of cyberbullying on others
- Technology specific sanctions for pupil engaged in cyberbullying behaviour could include limiting or refusing internet access for a period of time or removing the right to bring a mobile into school.
- Factors to consider when determining the appropriate sanctions include:
    - The impact on the victim: was the bully acting anonymously, was the material widely circulated and humiliating, how difficult was controlling the spread of material?
    - The motivation of the bully: was the incident unintentional or retaliation to bullying behaviour from others?

8.5 ‘Sexting’ and other exploitation, including grooming

Langenhoe Community Primary School ensure that all members of the school community are made aware of child exploitation via various technology.

- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Langenhoe Community Primary School views “sexting” and the above as a safeguarding issue and all concerns will be reported to and dealt with by The Head Teacher and action will be taken in line with the school safeguarding policy.

8.6 Radicalisation or Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

9. Communications Policy

9.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with pupils at the start of each year (see appendix 10 and 11 for e-safety posters for KS1 and KS2)
- Pupils will be informed that network and Internet use will be monitored
- E-safety will be included more prominently in e-safety lessons, as part of IPC and circle time.

9.2 Introducing staff to the e-safety policy

- All staff will be given the e-safety policy and its application and importance will be explained
- 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.

9.3 Enlisting parents' support

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- The school disseminates information to parents relating to e-safety where appropriate in the form of:
    - Information and celebration evenings
    - Posters
    - Website/VLP – Web Anywhere
    - Newsletter items
    - Web Anywhere training
    - Purplemash training
    - E-Safety Workshops
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school (see appendix 3).
- 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) (see appendix 4)
- 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.

10. Equal Opportunities

Pupils with additional needs

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.
Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children.

11. Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the e-safety officer any issue of e-safety that concerns them.
This policy will 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 Central Government change the orders or guidance in any way.

Appendix 1

Langenhoe Community Primary School Acceptable Use Agreement:

Staff 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 Alice Badman school e-safety coordinator.

- 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 SIMS) 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 install any hardware of software without permission of Alice Badman
- 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 not use social networking sites on school computers and will not accept 'Friend Requests' from pupils currently attending the school. I understand the school strongly advises against accepting 'Friend Requests' from past pupils or parents associated with the school.
- 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.

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)

Appendix 2

Langenhoe Community Primary School
Acceptable Use Agreement:

Governor
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 governors are aware of their professional responsibilities when using any form of ICT. All governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Alice Badman school e-safety coordinator.

- I will only use the school's Internet/ Intranet 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 ensure that personal data (such as data held on SIMS) 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 install any hardware of software without permission of Alice Badman
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of 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 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 not use social networking sites on school computers and will not accept 'Friend Requests' from pupils currently attending the school.
- I will not use inappropriate references about the school or its staff and will never use pupils names on social networking sites.
- 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.

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: ……..

Langenhoe Community Primary School
Acceptable Use Agreement:

Primary Pupil Acceptable Use
E-safety Rules/Responsible use of Laptops, iPads and Purple Mash

- ✓ I will only use ICT in school for school purposes.
- ✓ I will ask permission before entering any website, unless my teacher has already approved that site.
- ✓ I will only use my own login and password, **which I will keep a secret.**
- ✓ I will only use my own school email address when emailing.
- ✓ I will only e-mail people I know, or my teacher has approved.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will only open/delete my own files.
- ✓ 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 unpleasant or nasty. If I accidentally find anything like this I will use Hector Protector to shut down the screen and tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will not use Internet chat except if it is a discussion room that has been set up by my teacher.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Appendix 4

Primary Pupil Acceptable Use

E-safety Rules/Responsible use of laptops, iPads and Purple Mash.

Please complete, sign and return to the school office

Child's Name:

Pupil's Agreement

I have read and understand the school e-safety rules and Rules for Responsible use of laptops, iPads and Purple Mash. I will use laptops, Purple Mash and the Internet in a responsible way and obey these rules at all times. In particular, I will not share **my password with anybody else**. **I will not give out my name, home address or phone number** in email messages or write messages that I would not let my teachers and parents read. If I receive an e-mail which upsets me or an e-mail from somebody I don't know, I will tell my teacher or parents immediately.

Signed: Date:

Parent's Consent for Internet Access to Laptops, Purple Mash and iPads

I have read and understood the school rules for responsible use of laptops, ipads and Purple Mash. I give permission for my son / daughter to access this via the Internet. 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, however have precautions to help keep the children safe (for example Hector Protector).

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

I will try to ensure that my child understands the importance of keeping their password a secret.

Signed: Date:

Parent's Consent for Web Publication of Work

I agree that my son/daughter's work may be published on Purple Mash.

Signed: Date:

Appendix 5
Langenhoe Community Primary School
Photo Permission form

Throughout your child's time at Langenhoe, they child will participate in activities, events or projects in which they may be photographed. This includes class projects, school portraits, plays, trips or special events. Please fill out this form and return to the office by Friday 20th September.

Child's Name: _____

I consent to my child being photographed by:

- An official photographer
- Their class teacher

I consent to my child's photo being used in the following ways:

- On the school web site
- On Purple Mash (Secure Website which only the school Accesses)
- 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)

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

The school understands that many parents enjoying sharing photos of their children and their friends at school events through social networking sites (such as facebook). However the school asks that parents only take photos of their own children at these events.

Please sign one of these options:

I agree to all of the above statements:

Signature ……..…… Date …… (parent/carer)

Full Name …….....(printed)

If you do not agree with any of these statements please, state which statement/s and your child will be opted out:

Signature …….…… Date …… (parent/carer)

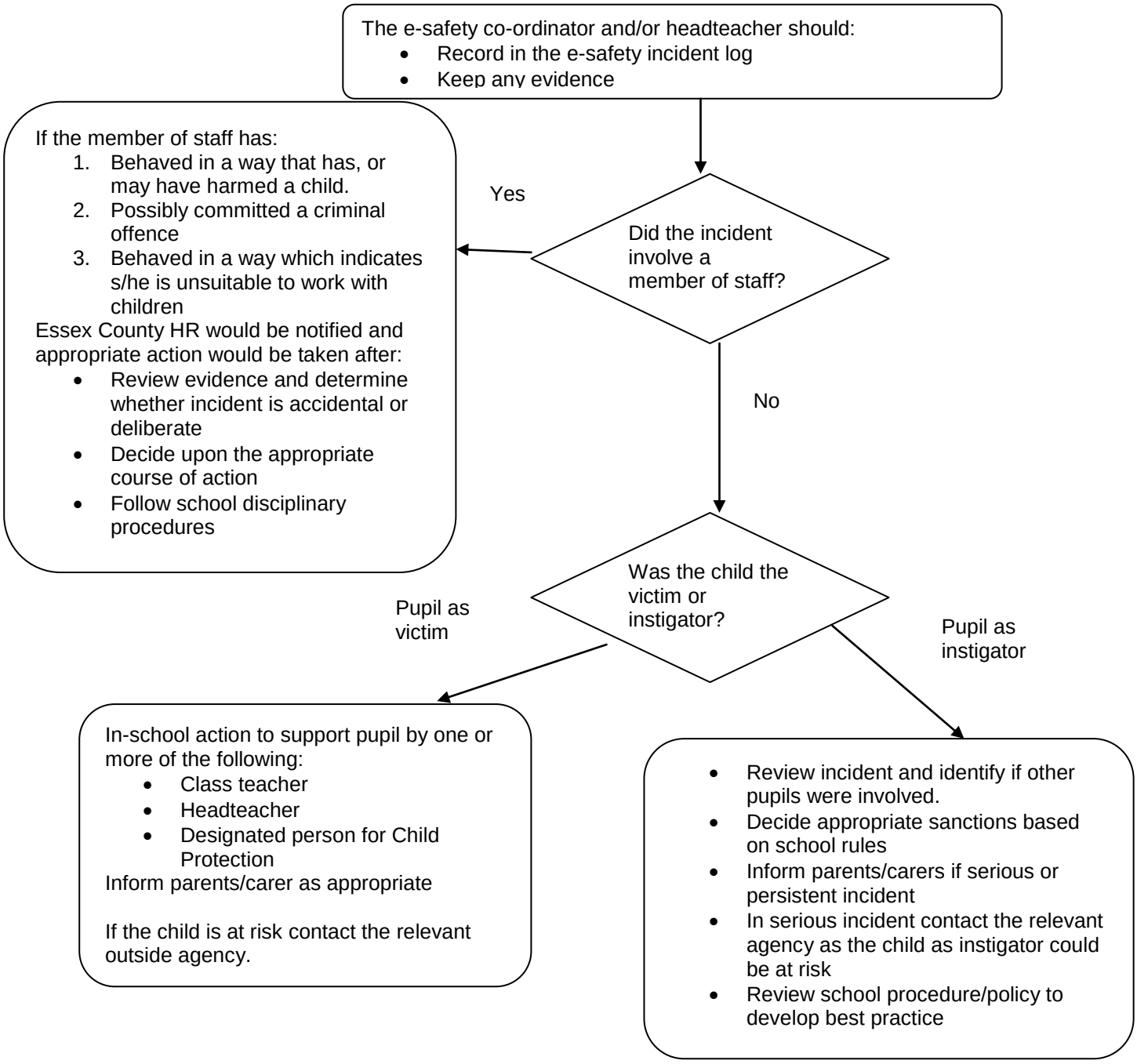
Full Name …….....(printed)

Appendix 6

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

Incidents not involving any illegal activity, such as:

- using another persons 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)

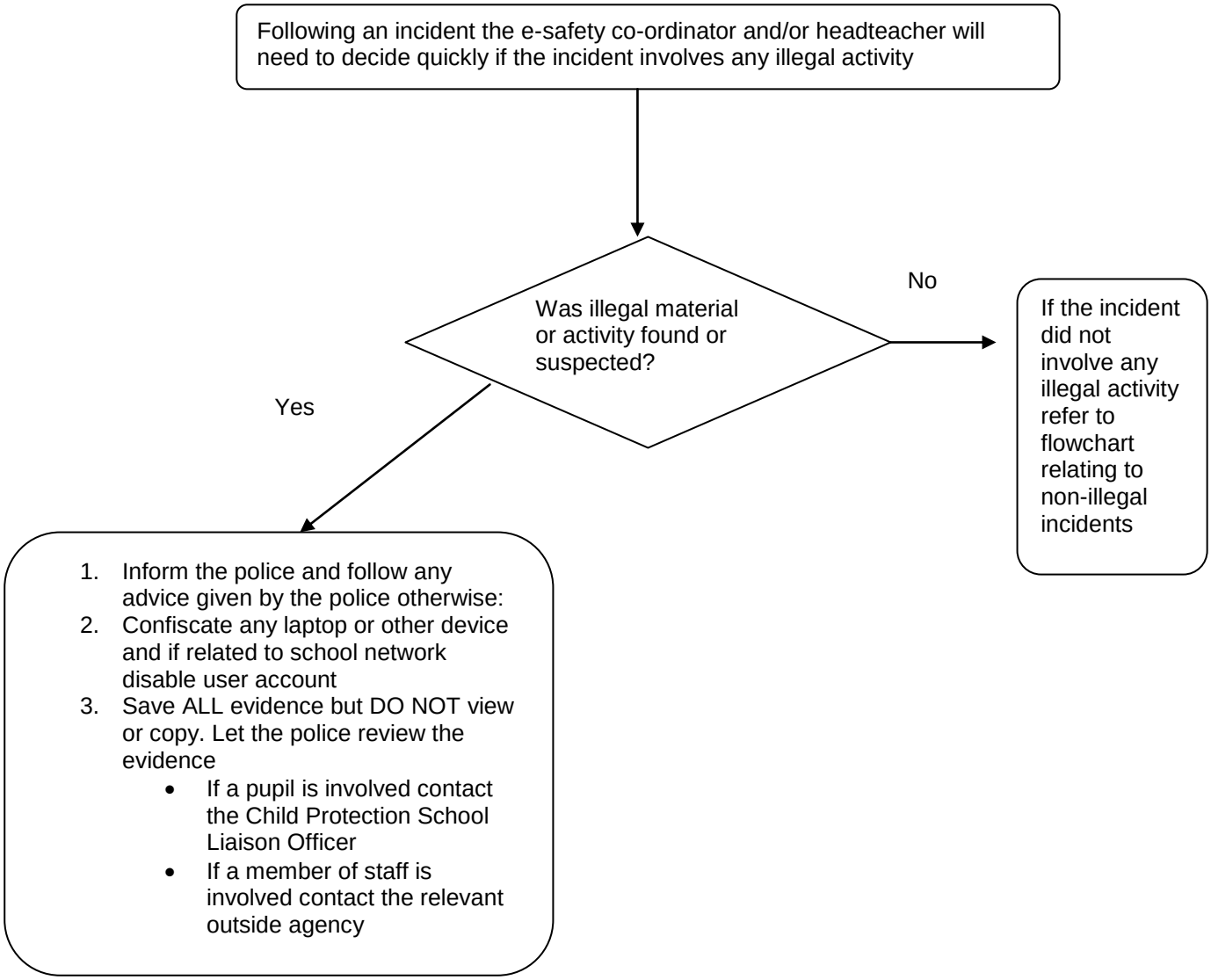


Appendix 7

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 8

Langenhoe e-safety Incident Log

Details of ALL e-safety incidents to be recorded in the Incident Log by the e-safety co-ordinator. This incident log will be monitored termly by the e-safety co-ordinator and 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 9

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.

- Always tell someone else: a teacher, youth worker, parent, or carer. Get them to support you and monitor what's going on.
- 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 don't 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 were 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 chat room.
- 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.

Appendix 10

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.

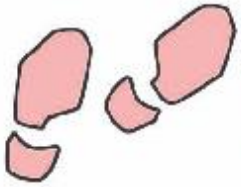
These rules help us to stay safe on the Internet

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