

E-Safety and Acceptable Use of ICT Policy

Clarity Independent School

Bridge Barn Farm
Woodhill Road
Sandon
CM2 7SG

Clarity Independent School is committed to safeguarding...

"Our school is committed to our whole-school approach to safeguarding, which ensures that keeping children safe is at the heart of everything we do, and underpins all systems, processes and policies...We promote an environment where children and young people feel empowered to raise concerns and report incidents and we work hard in partnership with pupils, parents and care-givers to keep children safe."

Clarity Safeguarding Policy September 2022

Written by Debbie Hanson
Head Teacher and Proprietor

This is version [4]
Written on: 18.6.19
Updated / Date: 7.12.22
Name: S. Ailara

1. Introduction

At Clarity Independent 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.

Clarity Independent 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 written by the Head Teacher and is contributed to by the whole school; pupils and staff.

For expectations regarding the taking, distribution and publication of photography and other media at Clarity Independent School see the Photography Consent Form This policy is to be read in conjunction with all other policies particularly:

- Behaviour Policy
- Child Protection and Safeguarding Policy
- Child on Child Harmful Sexual Behaviour Policy
- Antibullying Policy
- Code of Conduct policy (in teachers' handbook)
- Photograph Consent Form Policy
- Equality Policy
- CCTV and Media Policy

Whole school E-Safety and acceptable use of ICT training takes place during assemblies (morning meetings), ICT and PSHCE & RSE lessons.

2. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in Clarity Independent School. All staff members receive E-Safety online training from Educare, as part of their induction and sign an agreement of code of conduct.

Mrs S.Ailara (Deputy Head Teacher) has overall responsibility of e-safety. Children can report any concerns to class teachers.

It is the role of these staff members to keep abreast of current issues and guidance through organisations such as Enfield LA, Becta, CEOP (Child Exploitation and Online Protection), “The two Johns” (EST) E-Safety training and Child Net. Regular training will also be given at the school and online via the Educare annual training platform, along with “The two Johns” (EST) E-Safety training.

The Deputy Head Teacher ensures all staff are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

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

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community (see appendices)
- their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff receive information on the school’s acceptable use policy as part of their induction. Temporary Teachers and all staff must sign an acceptable use of ICT agreement before using technology equipment in school (see page 12 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 are prominently displayed in class teaching areas.
- Half-termly E-safety newsletters are emailed to parents (and are also on our website) sharing tips, fact-sheets and information on new games/apps to support parents’ understanding of current online trends amongst children, and to promote open discussions about E-safety between children, parents and adults in school.

3. Curriculum

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

- We provide opportunities within a range of curriculum areas to teach about e- safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the ICT and RSE curricula.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the ICT and RSE curricula.
- We periodically distribute questionnaires to children to monitor their understanding of e-safety. Please see appendices.
- Pupils are aware of the impact of online bullying through PSHCE & RSE 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
- We promote a 'Safe to talk' non-judgemental culture within school (and at home with parents) to encourage pupils to feel able to talk openly about their online experiences and disclose any 'unsafe' or worrying online experiences.

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 re-check these sites and supervise any further research.

Our internet access is controlled through:

**School secure FTTC web filtering service,
provided by United Network Technologies.**

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

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety co-ordinator (Mrs S Ailara) and an email sent to the Business Manager, cc Mrs Hanson and the network manager (Danny Lagden at DL Solutions) with the link copied and pasted into the email, so that they can block the site.

It is the responsibility of the school, by delegation to the network manager (Danny Ladgen), 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 2018. 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 apart from the Office for monitoring and security purposes. All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy (see p12).

6. Emails

The use of e-mail within most schools and colleges is an essential means of communication for both staff and pupils. In the context of Clarity Independent School, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools and colleges on different projects, be they staff based or pupil based, within school / college or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

Managing Email

The school gives all staff their own school e-mail account to use for all school business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.



It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, e-mail histories can be traced. The school email account should be the account that is used for all school business.

Under no circumstances should staff contact pupils, parents or conduct any school or college business using their own or another **personal (non-school)** e-mail address.

All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Head Teacher, line manager or designated account.

Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their e-mail account as follows:

- Use a flag system to prioritise emails needing attention and set them apart from those dealt with
- Keep all previous emails as a record of communication

All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

Staff must inform the SLT if they receive an offensive e-mail.

Pupils are introduced to e-mail as part of the ICT Scheme of Work.

Access to the School's e-mail (whether directly, through webmail when away from the office or on non-school hardware) is always subject to the School's policies.

Sending Emails

If sending e-mails containing personal, assessment / performance, confidential, classified or financially sensitive data to external third parties (including parents / care-givers) or agencies, refer to the Section 'E-mailing Personal, Sensitive, Confidential or Classified Information'

Use own Clarity e-mail account so that you are clearly identified as the originator of a message.

Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

Clarity e-mail is not to be used for personal advertising / marketing.

Receiving emails

Staff are to check their e-mail first thing in the morning and straight after the children have gone home, every working day.

Never open attachments from an untrusted source; Consult ICT personnel first.

Do not use the e-mail systems to store attachments. Detach and save business related work attachments to the appropriate shared drive/folder.

The automatic forwarding and deletion of e-mails is not allowed.

E-mailing Personal, Sensitive, Confidential or Classified Information

Where e-mail is used to transmit such data:

- Obtain express consent from your manager to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
 - Encrypt and password protect using the Microsoft Outlook Sensitive External Email Encryption option. If you do not have access to this, our Business Manager will open a conversation with the recipient for this to be facilitated, alternatively, if you wish to send a secure email to Essex Local Authority, send a request for the recipient to send you a sensitive secured email thread, which you can reply to - your reply will be secure.
 - Verify the details, including accurate e-mail address, of any intended recipient of the information

- Verify (by phoning) the details of a requestor before responding to e-mail requests for information and check with SLT before sending
 - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
 - Copy Debbie Hanson in so as to be informed the information has been sent.
-
- Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
 - Send the information as an encrypted document **attached** to an e-mail via the Business Manager using Outlook External Email / Local Authority sensitive encrypted email system
 - Where a password is also used, provide the encryption key or password by a **separate** contact with the recipient(s) via outlook External Email/ LA sensitive encrypted email
 - Do not identify such information in the subject line of any e-mail
 - Use pupil's initials only
 - Request confirmation of safe receipt
 - If a parent sends you such data not using Outlook encryption, advise them of our policy and send an external encrypted email to their account (via Business Manager) in order for them to send personal information in future.

7. 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 Head Teacher. Incidents should be logged and the flowchart for managing an e-safety incident is to be followed (see appendices). 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 cyber-bullying incidents (as with all bullying incidents) should be recorded and investigated via the school safeguarding system; CPOMS.

8. Review of Policy

There are on-going opportunities for staff, children and families to discuss e-safety concerns with our staff. This policy needs to be reviewed every 2 years 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.

Appendices

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

Appendix 1 - Clarity Independent School Pupil Acceptable Use of ICT Agreement / E-Safety Rules

- ☐ I will only use ICT in school for school purposes and during lessons I will only use ICT for the intended purpose.
- ☐ I will only use my class e-mail address or my own school e-mail address when e-mailing.
- ☐ I will only open e-mail attachments from people I know, or who my teacher has approved.
- ☐ I will not tell other people my ICT passwords.
- ☐ I will only open/delete my own files.
- ☐ I will not bring software, CDs or ICT equipment into school without permission.
- ☐ I will only use the Internet after being given permission from a teacher.
- ☐ I will make sure that all ICT contact with other children and adults, both in and out of school, is responsible, polite and sensible.
- ☐ I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately if in school, or get help from an adult if at home.
- ☐ 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 unless this is part of a school project approved by a teacher and a responsible adult comes with me.
- ☐ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ☐ I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my e-Safety.

I (name) agree to follow this policy and understand that non-adherence to the above means that I will experience consequences, such as not being trusted to use ICT independently and losing my computer privileges.

Signed:

Date:

Appendix 2: To be agreed with parent upon child's admission to the school

Clarity Independent School
Bridge Farm Barn
Woodhill Road
Sandon
CM2 7SG

DATE

Dear Parents/Carers,

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

Please read and discuss with your child the E-Safety rules overleaf and return this sheet signed by both you and your child. If you have any concerns or would like some explanation, please contact your child's class teacher.

This Acceptable Use of ICT Agreement is a summary of our E-Safety and Acceptable Use of ICT Policy, which is available in full on our website or is available as a hard copy in our Office/Reception.

Yours sincerely,

Debbie Hanson, Head Teacher

Pupil: I have read, understood and agreed with the Rules for Acceptable use of ICT.

Signed (child) Date.....

Parent's/Carer's Consent for Internet Access

I have read and understood the school rules for Acceptable Use of ICT and give permission for my son / daughter to access the Internet in school. 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.

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/carers) Date.....

Appendix 3 - Clarity Independent School Staff and Visitor Acceptable Use of ICT 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 Debbie Hanson, Head Teacher or a member of the Child Protection / Safeguarding team.

- I will only use school's email /Internet /Intranet /Learning Platform /any related technologies for professional purposes or for uses deemed 'reasonable' by the Head Teacher.
- I will comply with the ICT system security and not disclose or change 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 parents or 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 school records) 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 Teacher.
- 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 in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head Teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.

User Signature

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

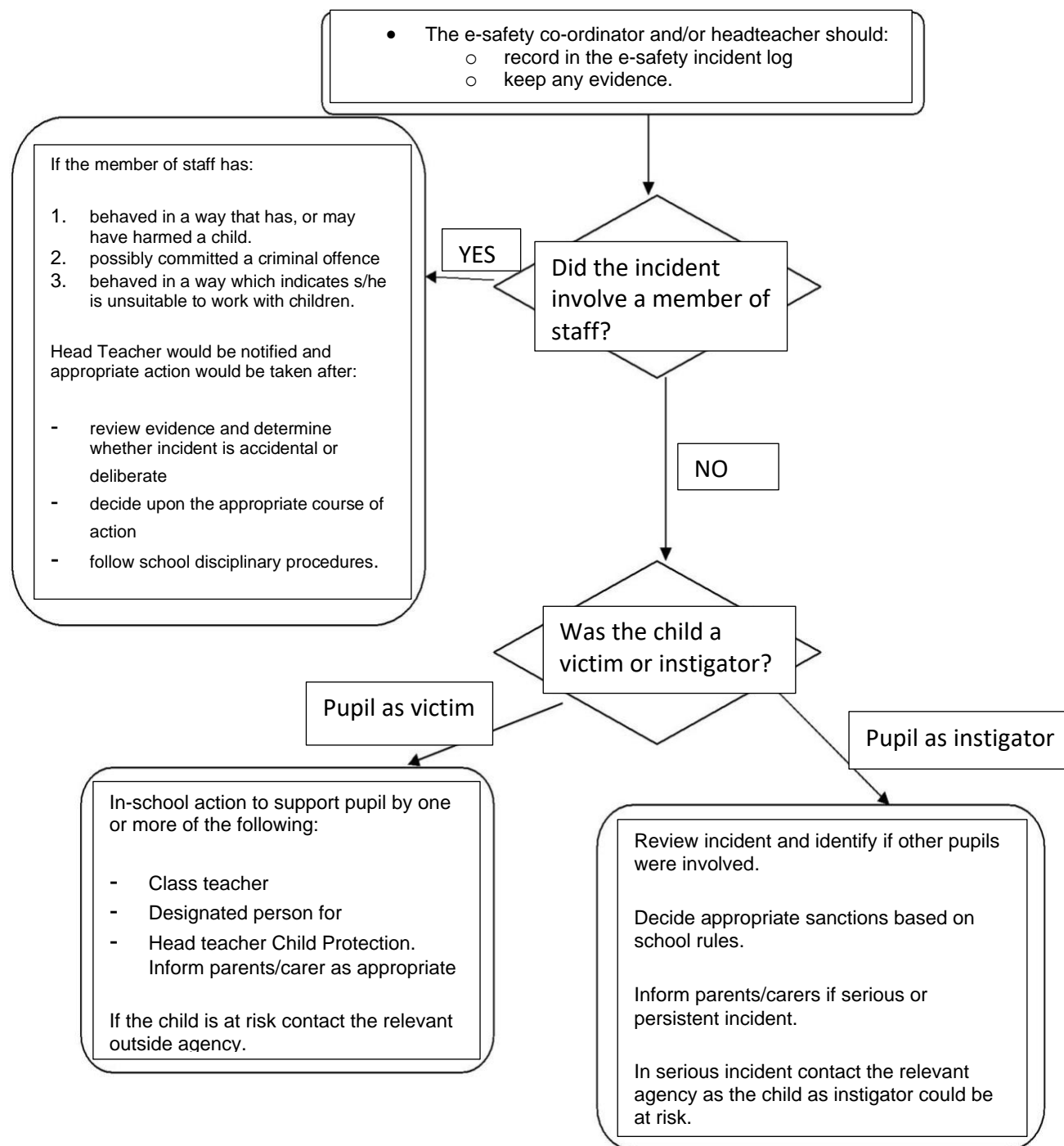
Signature Date

Full Name (printed) Job title:

Appendix 4 - Flowchart for Managing an e-Safety incident not involving any illegal activity

Incidents not involving any illegal activity, such as:

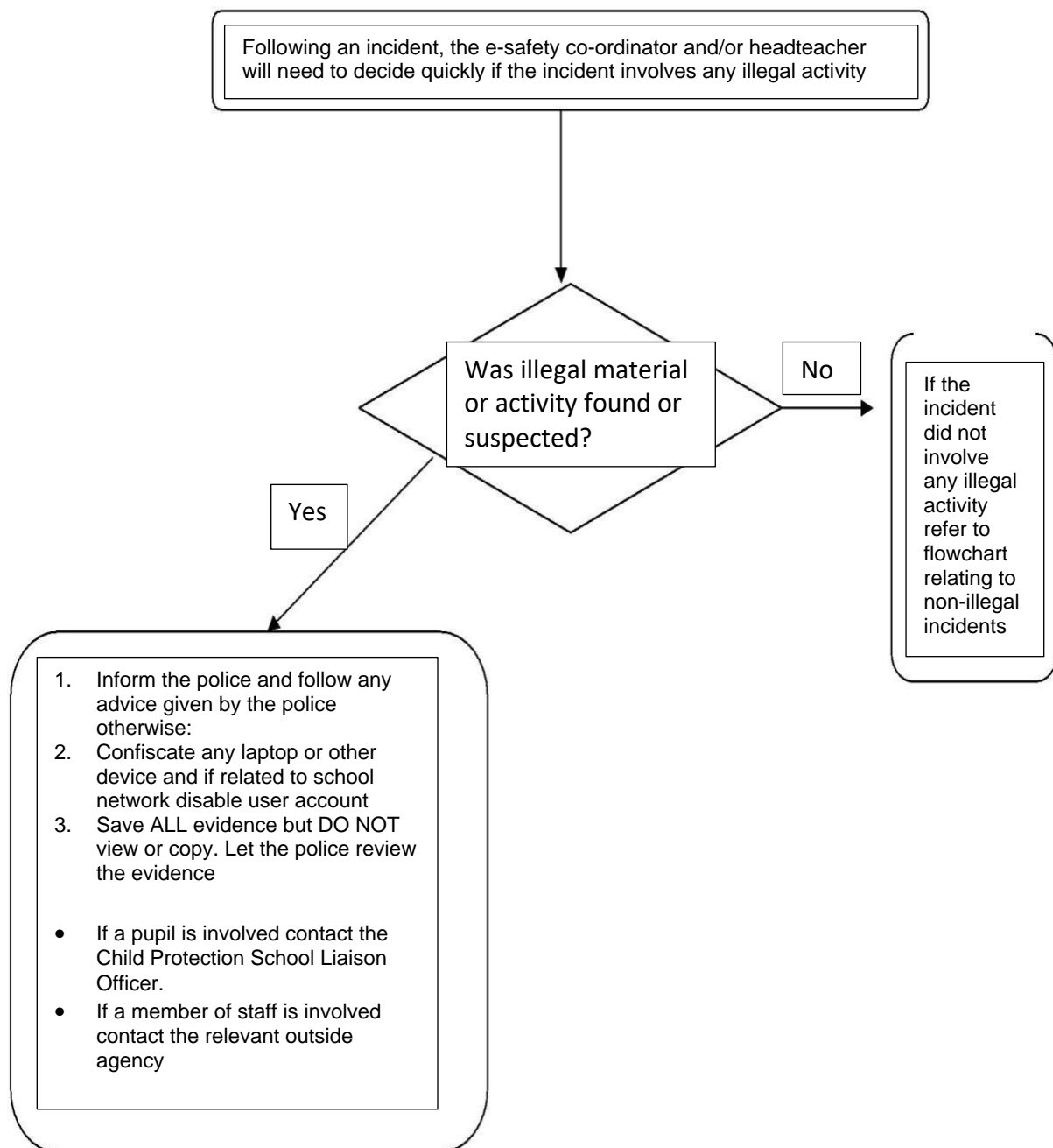
- using another person's user name and password
- accessing websites which are against school policy
- using a mobile phone to take video during a lesson
- using the technology to upset or bully (in extreme cases this could be illegal)



Appendix 5 - Flowchart for Managing an e-safety incident involving illegal activity

Illegal means something against the law, such as:

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



Appendix 6: Advice for Children on Cyber-bullying

If you're being bullied by phone or the Internet:

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

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

Text/video messaging

You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. To find out how to do this, visit www.wiredsafety.org.

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

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

Phone calls

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

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



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

Emails

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

Web bullying

If the bullying is on a website (e.g. Bebo) tell a teacher or parent, just as you would if the bullying was face-to-face – even if you don't actually know the bully's identity. Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging

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

Three steps to stay out of harm's way

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

Appendix 7 - Anti-Bullying & Cyber bullying questionnaire (younger pupils - orally)

Class.....

No. of pupils taking part

1. Does the word bullying mean;

Someone is unkind to you once.....

Someone is unkind to you more than once.....

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

.....

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

3. How many children did not know about the Clarity 6?

4. How many children use the internet at home?.....

5. How many of those children use the internet;

(a) Alone.....

(b) With an adult.....

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

.....

.....

(Please explain the importance of knowing either their address, post code or a contact number and put onto pupil learning plan to learn and practise)

Anti-Bullying & Cyber bullying Questionnaire

(Older pupils – written)

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

1. What does the word bullying mean to you?
2. What do the words Cyber bullying mean?
3. If you felt that you were being bullied in our school, what would you do?
4. If you felt that you were being bullied outside of school, what would you do?
5. Name two actions you could use from 'The Clarity Six'.
6. What is the 'Red Box' in our school used for?
7. What do the Mini Mentors do in our school? Where can you find them?
8. If you play games on the internet, do you play with people you don't not know personally?
9. Do you know how to report rude or bullying messages online?
10. Write either your home address or a telephone number you could call in an emergency.

Appendix 8 - 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.



Appendix 9: Younger pupils

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.


Older pupils


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

Appendix 10: Student Laptop Home-Use Agreement

The purpose of this form is to make sure your son or daughter gets the most from their laptop computer and printer (where applicable) from here on known as 'device' / 'equipment'. Please read the notes below, sign at the bottom to give your consent and return the form to school.

The School's E-learning Home-Use Scheme is open to all students on roll at Clarity Independent School. Parents may decide whether to opt into the scheme for their child or not on the basis of the conditions below.

- ❖ The provision of a device for a student is given on the understanding that the device is used with supervision and for educational purposes.
- ❖ The student must bring the device back into School following lockdown.
- ❖ The device remains the property of Clarity Independent School at all times.
- ❖ The School may charge parents for all or part of the costs of deliberate damage to, careless breakage or loss of the device provided to the student (please see the School's "Charging & Remission Policy").

We (parent and pupil) understand that:

- The equipment remains the property of the school.
- (I will bring my laptop to School fully charged every day, unless I have been told not to.)
- I am responsible for the equipment including all its components. I will not leave it unattended; I will protect it from possible damage; I will not loan it to others; I will only carry the laptop around in its special laptop case, whether or not this is inside another school bag; I will not decorate / customise the equipment or case.
- I will make sure the computer is not used for any illegal and/or anti-social purpose, including access to inappropriate internet sites and chat rooms.
- If the equipment is lost or stolen outside School, the School must be notified immediately. The police must be informed and a crime reference number obtained to give to the school's Network Manager.
- If I no longer wish to use the equipment, I will notify and return it to the school in a timely manner, which has, in advance, been agreed with the school, so that another student can benefit.
- Wilful / careless misuse of part / whole of the equipment may result in it being recalled by the school.
- I will report any damage or faults promptly. The School may charge parents for all or part of the costs of deliberate damage to, careless breakage or loss of the device(s) provided to the student (please see the School's "Charging & Remission Policy").

Laptop value: ____£350_____

Printer value if applicable: ____£100_____

I (parent) confirm that I have read and understood the items above and discussed this with my son/daughter. I confirm that I will supervise my son / daughter at all times when using the internet and computer to reduce the risk of exposure to inappropriate material.

Parent /carer name: _____
(print name and surname in full)

Student's name: _____
(print name and surname in full)

Parent/carers signature: _____

Student signature: _____

Date: _____

Date: _____