St Barnabas CE Primary School

E-safety Policy

Approved by:
The Board of Governors

Date: 25th January 2017

Last updated: 20 January 2017

Contents:

Statement of intent

At St Barnabas, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. Technology is also embedded in our day-to-day lives through many different types of devices and platforms.

As technology is constantly developing, we endeavour to stay up-to-date with current issues around the use of technology and how they can affect young people.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use. There is an ever-growing need for better filtering and monitoring of what pupils can access both in school and at home through the use of firewalls and monitoring software. We also acknowledge a greater need for this to be shared to all members of the wider school community, including staff, pupils and parents alike.

E-safety includes, but is not limited to, browsing the internet. Other forms of electronic communication and interaction such as e-mail, blogging, social networking and online gaming should be considered as well as the corruption, misuse, hacking and publication of personal data.

When using the internet, young people need to be protected from dangers including violence, racism and exploitation. Much of the material on the Internet is published for an adult audience and therefore may be unsuitable for pupils. They need to learn to recognise and avoid any potential risks – to become "Internet Wise". Pupils need clear guidance in order to prepare them to respond appropriately to any situation, using any of the previously mentioned methods of electronic communication, for the inevitable moment when they come across inappropriate material or find themselves in an uncomfortable situation.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

Named E-safety Officer: Sam Hazeldine

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998
- The Regulation of Investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

1.2. This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping Children Safe in Education'

2. Using the internet safely

2.1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools to implement, which minimise harmful risks.

2.3. The school uses an LA-monitored firewall which restricts and filters the access that pupils have to the internet. A separate log-in is used for staff.

2.4. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of the [school], and to deal with incidents of such as a priority.

3.2. The e-safety officer, is responsible for ensuring the day-to-day e-safety in our school, and managing any issues that may arise.

3.3. The headteacher is responsible for ensuring that the e-safety officer and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

3.4. The e-safety officer will provide relevant regular training and advice for members of staff on e-safety. They will ensure training is up-to-date.

3.5. The headteacher will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

3.6. The e-safety officer will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.

3.7. The school will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.8. The e-safety officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

3.9. The e-safety officer will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.

3.10. The e-safety officer will ensure all aspects of e-safety are taught regularly throughout the computing curriculum through monitoring of assessment and planning.

3.11. Cyber bullying incidents will be reported in accordance with the school's Anti-bullying and Harassment Policy.

3.12. The governing body will hold regular meetings with the e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

3.13. The governing body will evaluate and review this E-safety Policy on at least an annual basis, taking into account the latest developments in ICT and the feedback from staff/pupils.

3.14. The headteacher will review and amend this policy with the e-safety officer, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

3.15. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.16. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.17. All staff and pupils will ensure they understand and adhere to our Acceptable Use Policies, which they must sign and return to the headteacher.

3.18. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

3.19. The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

4. E-safety control measures

4.1. Educating pupils:

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Our teachers understand that they have a role to deliver and implement the teaching of e-safety so that it is effective and memorable. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- All Classes will be taught 'Rules for Responsible Internet Use', at the beginning of a school year, and the skills needed in order to use the Internet appropriately. Children in all classes will sign an agreement to use the internet appropriately and responsibly, as they have been taught to.
- The school will hold an annual e-safety week where the whole curriculum focuses on areas around internet safety.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms and revisited often by staff (see SMART poster – appendix 1)
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- Pupils will be made aware of the dangers of the use of technology
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school (see appendix 2&3)
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

4.2. Educating staff:

- All staff will undergo e-safety training on at least an annual basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.
- All staff will undergo audits by the e-safety officer in order to identify areas of training need.

- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.3. Educating Parents and the wider community:

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities – displayed on the school website.
- Letters, newsletters, web site
- Parents/Carers evenings/sessions
- High profile events/campaigns eg Safer Internet Week.

5. Internet Access

5.1 General internet use:

- Parents will be made aware of the acceptable use policy and will be asked to give their permission for their child to use the internet at school within the agreed policy.
- All users in key stage 2 have usernames and passwords for various subscriptions to school learning websites. They are encouraged to keep these confidential and talk to a member of staff if they feel their information is no longer secure or should be changed.
- Teaching staff will closely monitor children's internet activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to particular websites.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- The master users' passwords will be available to the headteacher for regular monitoring of activity.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the e-safety officer for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and no personal devices. This will be dealt with following the process outlined in section 8 of this policy – 'misuse by staff'.

5.2 Email:

- Staff will be given approved email accounts and are only able to use these accounts.
- Use of personal email to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via unsecure email. Security-validated CYC email accounts must be used for this.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

5.3 Social networking:

- Use of social media on behalf of the school will be conducted following the processes outlined in our Social Media Policy.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.
- Pupils are regularly educated on the implications of posting personal data online, outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught.

5.4 Published content on the school website and images:

- The headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the school website will be the phone, email and address of the school. No personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with the code of conduct in terms of the sharing and distribution of such.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

5.5 Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the e-safety officer.

- The e-safety officer must ensure that the filtering of websites and downloads is up-to-date and monitored.

6. Managing mobile technologies

Small wireless devices provide more opportunities for pupils to be exposed to content within school that cannot be controlled or filtered through the school network or security systems. This can even extend to games consoles used in after school care clubs where it is possible to connect to global gaming networks and interact with other people. At all times we need to be aware of the current technology and its possible risk and educational benefit.

- Pupils are not permitted to bring mobile phones or other electronic devices that have internet access into school. However, the headteacher may authorise the use of mobile phones by a pupil where parents/carers have requested it for safety or precautionary use.
- The use of cameras in mobile phones is not permitted.
- A blog may only be used in school by pupils if it is appropriately moderated.
- The school will ensure its wireless network will block connections from devices that are not part of its domain. (Personal laptops, IPads, iPod touches, wireless mobiles)
- Mobile devices are not permitted to be used during school hours by pupils or in teaching hours by members of staff.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the e-safety officer when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

7. Cyber bullying

7.1. For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

7.2. The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

7.3. The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

7.4. Parents are regularly sent information that defines cyber-bullying along with information of spotting the signs.

7.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils. This will include signage and information displayed around school to provide constant reminders and awareness of the issue.

7.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-bullying and Harassment Policy.

7.7. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

8. Reporting misuse

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

8.1 Misuse Procedure

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the e-safety officer and headteacher,
- Teaching staff should have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- The incident is written in the 'Incident log', kept by the e-safety officer.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse).
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher and will be issued once the pupil is on the [school] premises.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection Policy.
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not.

8.2 Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher.
- The headteacher will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

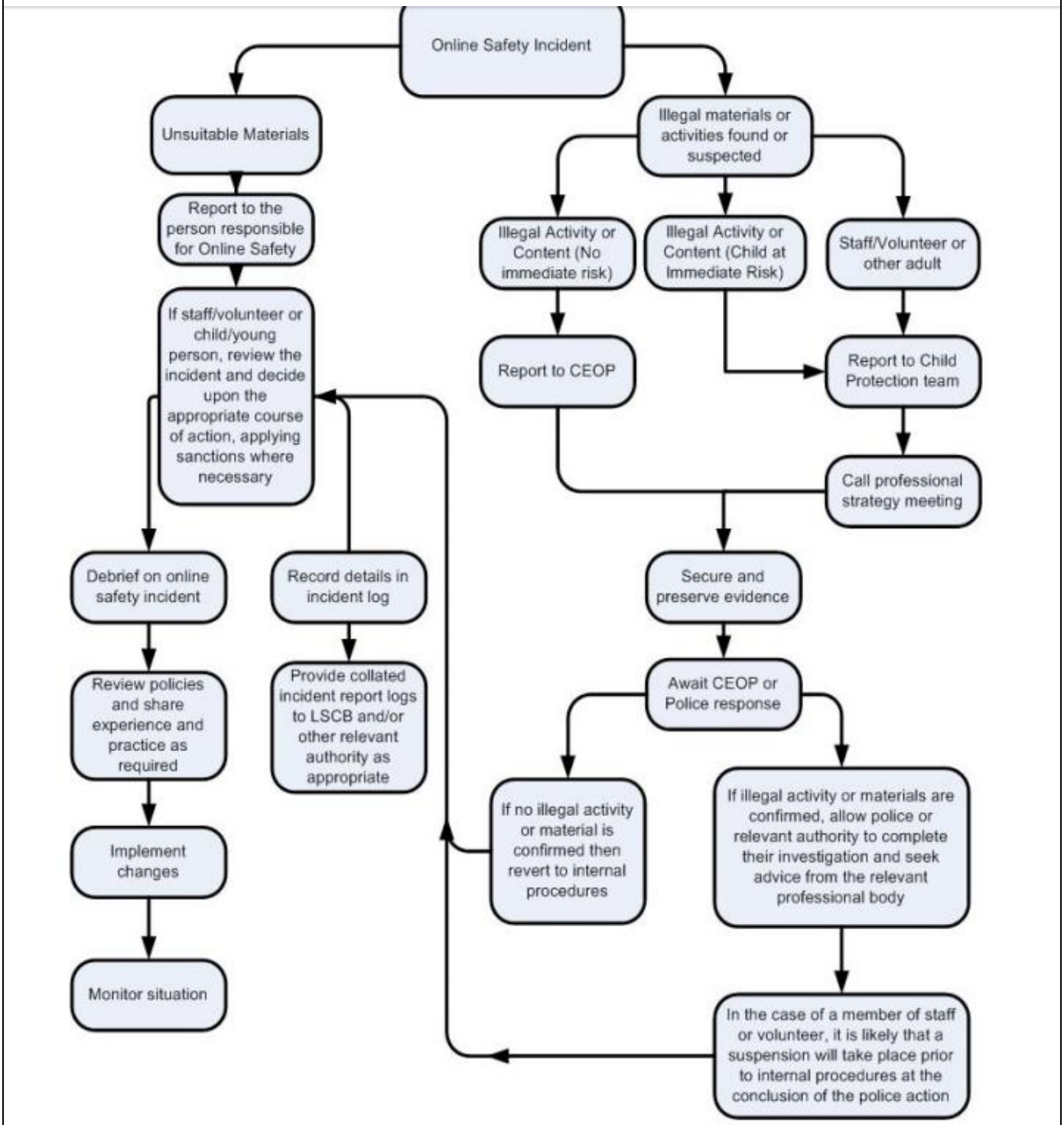
8.3 Further action:

If it is deemed necessary then appropriate action will be required and could include the following:

- Internal response or discipline procedures.
- Involvement by Local Authority or national/local organisation (as relevant).
- Police involvement and/or action.
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

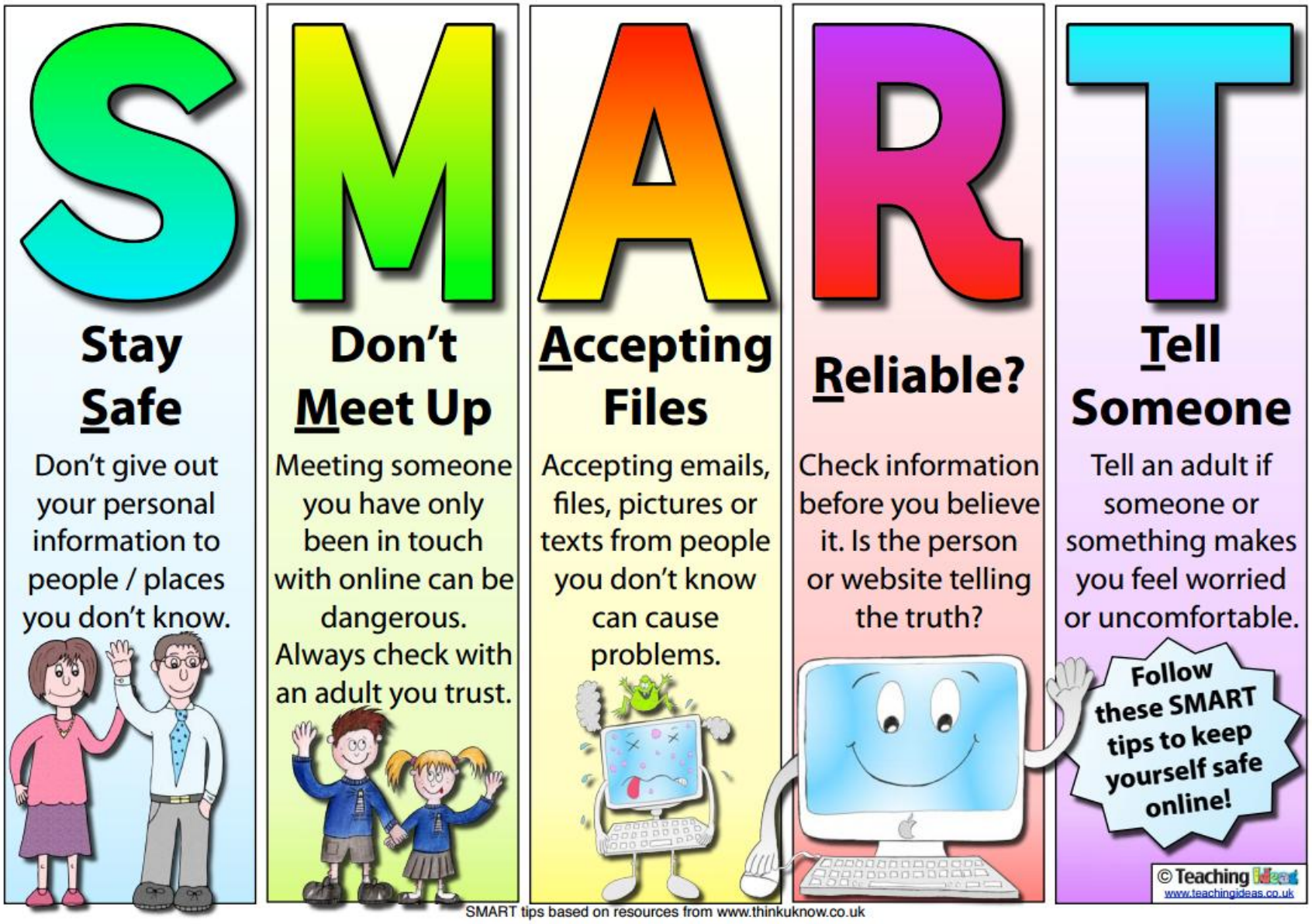
8.4 Model for dealing with illegal activity:

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Appendix 1

SMART poster displayed in classrooms.



SMART tips based on resources from www.thinkuknow.co.uk

Appendix 2

St Barnabas CE Primary School

KS2 Pupil Acceptable Use of ICT

- ☑ I will only use ICT in school for school purposes.
- ☑ 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 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.
- ☑ 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.

Appendix 3

St Barnabas CE Primary School

KS1 Pupil Acceptable Use of ICT

- ☑ I will ask an adult before I use a computer
- ☑ I will ask before I print.
- ☑ I will use the Internet, in a safe and responsible way by following instructions
- ☑ I know that the adults in school can check my files and website that I have visited
- ☑ If the adults in school have concerns about my safety they may contact my parents/guardian.
- ☑ If I have a problem, I always ask an adult.
- ☑ I understand that these rules are there to help me, my friends and my family feel safe.
- ☑ I will not share information about myself at home

I agree to follow these rules. If I break any of these rules I may have a consequence.

<u>Appendix 4 – Guidance for parents</u>
(also see online safety section of school website)

E-safety tips for Parents of Primary School Children

79% of 7-11 year-olds said they would tell their parent or carer if something worried them online.

Childnet, Have your Say (2013)

Checklist

Put yourself in control
Make use of the parental controls on your home broadband and any internet-enabled devices. You can find out how at your broadband provider's website or by visiting internetmatters.org.

Search safely
Use safe search engines such as swiggle.org or kids-search.com. Safe search settings can also be activated on Google and other search engines as well as YouTube. You can find out more at google.co.uk/safetycentre.

Agree boundries
Be clear what your child can and can't do online – where they can use the internet, how much time they can spend online, the sites they can visit and the type of information they can share. Agree with your child when they can have a mobile phone or tablet.

Explore together
The best way to find out what your child is doing online is to ask them to tell you about it. Put the family computer in a communal area so you can see what sites they're visiting and share with them.

Check if it's suitable
The age ratings that come with games, apps, films and social networks are a good guide to whether they're suitable for your child. The minimum age limit is 13 for several social networking sites, including Facebook and Instagram.

Know this stuff matters, but don't know where to turn?

Internet Matters is a free online resource for every parent in the UK. We'll show you the best ways to protect your children online – with information, advice and support on all the big e-safety issues.

internet matters.org

Appendix 5 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 coordinator and Head teacher.

Date & time	Name (Pupil/staff member)	Gender	Room and Device number	Details of incident	Action taken

Appendix 6

Advice for Children on Cyber-bullying (shared with KS2 classes)

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

Emails

- Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.
- Keep the emails as evidence. And tell an adult about them.
- Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. abuse@hotmail.com
- Never reply to someone you don't know, even if there's an option to 'unsubscribe'. Replying simply confirms your email address as a real one. Web bullying If the bullying is on a website (e.g. Bebo) tell a teacher or parent, just as you would if the bullying was face-to-face – even if you don't actually know the bully's identity. Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging

- Never give out your name, address, phone number, school name or password online.
- It's a good idea to use a nickname. And don't give out photos of yourself.
- Don't accept emails or open files from people you don't know. Remember it might not just be people your own age in a chatroom.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.
- Think carefully about what you write; don't leave yourself open to bullying.
- Don't ever give out passwords to your mobile or email account. Three steps to stay out of harm's way
- Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.
- If someone insults you online or by phone, stay calm – and ignore them.
- Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else.