"Nurturing a lifelong love of learning"

Chapel Allerton Primary School

Online Safety Policy and Acceptable Use of Computing Agreements

September 2025
Review date: September 2027

Introduction

At Chapel Allerton Primary School we understand the responsibility we have to educate our pupils and staff about online safety issues. It is important to teach appropriate behaviours and critical thinking skills to enable everyone to remain safe and legal when using the internet and related technologies in and beyond school. It is important to teach how to communicate respectfully online and how to react to and report harmful content.
Chapel Allerton Primary School has a whole school approach to the safe use of computing. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into **four areas** of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

This policy is to be read in conjunction with all other policies particularly Chapel Allerton Primary School's: Safeguarding and Child Protection Policy, Behaviour and Relationship Policy, Anti-Bullying Policy and Acceptable Use of Computing Agreement for Staff as well as considering the principles of the Safer Working Practice Guidance (National Safer Recruitment Consortium) as well as guidance from the Department for Education (Safeguarding Children in a Digital World), CEOP (Child Exploitation and Online Protection) and Communication Act 2003 (Section 127 Improper Use of Public Electronic Communications Network).

http://www.legislation.gov.uk/ukpga/2003/21/section/127

Roles and Responsibilities

Online safety is recognised as an essential aspect of safeguarding all children in Chapel Allerton Primary School. All staff members are expected to appropriately respond to any online safety issues and alert our designated safeguarding staff (Mr Sykes and Miss Robbins) of any concerns as necessary.

It is the role of our computing subject leader and designated safeguarding staff to keep up to date with current online safety issues and guidance through the DfE, Leeds City Council alerts, and information shared by national organisations such as Child Exploitation and Online Protection (CEOP) and the NSPCC. The Head Teacher ensures that the senior leadership team and Governors are updated as necessary. These messages are then passed onto parents and carers appropriately to ensure they are aware of these concerns at home. All teachers are responsible for promoting and supporting safe behaviours when using the internet in lessons and follow school online safety procedures.

All staff are required to sign school's Acceptable Use of Computing Agreement regarding:
• safe use of e-mail
• safe, professional and responsible use of mobile phones, the internet and social media.
• publication of pupil information/photographs on the school website and the school's social media.
• procedures in the event of misuse of technology by any member of the school community.

Staff are reminded/updated about online safety regularly and new staff receive information on the school's acceptable use of computing as part of their induction. Staff are solely responsible for any content on their own personal social media networks and electronic devices. This means that staff are responsible for managing their own applications and content to ensure that it is always professional and appropriate. (See appendix 2)

Teaching, Learning and School Culture

Chapel Allerton Primary School has a duty to provide pupils with quality, safe internet access as part of their learning journey. Internet use is a necessary tool for staff and pupils and will enhance learning. We believe it is essential for online safety guidance to be given to the pupils on a regular, progressive and meaningful basis.

At Chapel Allerton Primary School, the pupils learn, or develop a culture of keeping safe online, through:

- Timetabled and structured Online Safety lessons taught explicitly as part of the Computing curriculum (See Progression of Skills in Computing document). Lesson content includes secure passwords, personal information, online kindness, understanding age-appropriate content, trust, downloading content, reporting concerns, posting content, commenting appropriately, managing time online.
- Our PSHE curriculum
- Our MindMate curriculum
- Regular Online Safety Assemblies
- Regular classroom discussions and circles
- Safer Internet Day activities
- Pupil Voice Discussions with the Computing Subject Leader

Creating images of pupils through photography and video

Many work-based activities involve recording images, and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. However, written consent should be obtained from legal guardians prior to creating any images of children (See Appendix 9).

Staff must be clear about the purpose of the activity and about what will happen to the images when the lesson/activity has concluded, be able to justify images of pupils in their possession and avoid taking images in one-to-one situations. Photograph or video images of pupils will be created using equipment owned or provided by school.

School Website, Social Media and Parental Engagement

Chapel Allerton Primary School only publish images of pupils with prior consent from their legal guardian. We do not share staff or pupil personal information. The Head Teacher and Deputy Head Teacher will take overall editorial responsibility and ensure that published content is accurate and appropriate. Guardians are invited to Online Safety meetings to learn about, and share thoughts on, Online Safety with the Computing subject leader and the school's Wellbeing Officer.

The school website includes:

- A half termly school timetable of Computing lessons including Online Safety
- Chapel Allerton Primary School's Child Friendly (School Council) Online Safety Policy
- Online Safety newsletters to guardians

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 pupils. Pupils 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

Commented [MW1]: Do we definitely have these? Might be CT question

Commented [TR2R1]: I have asked CT and BP to review this bit

Commented [cT3R1]: There is a timetable on the website - it does need updating but I'm waiting for Purple mash to fully release their modules first before we change things around

Commented [cT4R1]: Newsletters I usually post on class dojo half termly but can also upload to the website too

with pupils.
If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research.
Our internet access is controlled through Talk Straight, this has firewalls and filtering included (filters web content).
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 class teacher and an email or help desk ticket sent the ICT Technician so that the site can be blocked.
It is the responsibility of the school, by delegation to the ICT technician, 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 our ICT technician and senior leadership team.

Inappropriate material
When considering what is defined as inappropriate material, it is important to differentiate between inappropriate and illegal and inappropriate but legal. All staff should be aware that in the former, case investigation may lead to criminal investigation, prosecution, dismissal, and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

Material which incites hate, harm or harassment
There are a range of offences in relation to incitement of hatred based on ethnicity, religion, gender, sexual orientation, or similar grounds, and particular offences concerning harassing or threatening individuals which includes cyber bullying by mobile phone and social networking sites etc. It is an offence to send indecent, offensive, or threatening messages with the purpose of causing the recipient distress or anxiety.

Social media, Online gaming, Apps and Websites
The school recognises that there is an ever-growing development of social media apps and online games (such as TikTok, Snapchat, Roblox, Instagram) that pupils may be able to access at home. As part of the curriculum, we will ensure that pupils understand how to keep themselves safe online. At home, it is the responsibility of parents/carers to monitor the games/apps that their children are accessing. The school will support parents by providing up to date online safety information via paper, electronic and face to face communications.

Security and Data Protection
The school and all staff members comply with the Data Protection Act 2018 including the European Union's General Data Protection Regulation (GDPR). Personal data will be recorded, processed, transferred, and made available according to the act.

Confidentiality
Members of staff may have access to confidential information about pupils, children and young people and the organisation to undertake their everyday responsibilities and in some circumstances, this may be highly sensitive or private information. Such information should never be shared with anyone outside the school, a member of the public or outside agencies, except in specific circumstances, for example when abuse is alleged or suspected. In such cases individuals have a duty to share information without delay, but only to those with designated child protection responsibilities or a senior member of staff.
Password security is essential for staff and secure passwords must not be shared with anyone. Confidential information should never be stored on personal computers or devices or distributed through personal e-mail or internet channels. Only authorised school-based devices and systems should be used to store and transfer confidential information.

For further guidance in relation to confidentiality issues and safe storage of data

please refer to the Guidance for Safer Working Practice February 2022 or speak with school's Business Manager (Miss Walter).

Online Safety Complaints/Incidents

As a school we take all precautions to ensure online 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. Senior Leaders should be notified of any complaints from pupils, staff or parents/guardians. If further investigation is required, then the school's ICT Technician may become involved and act or consult with Talk Straight web filtering service as necessary. Incidents should be logged and the flowchart for managing an online safety incident is to be followed. It is important that the school work in partnership with pupils and parents to educate them about cyber bullying and children, staff and families need to know what to do if they or anyone they know are experiencing cyber bullying. All bullying incidents should be recorded on CPOMS and investigated by the Senior Leadership Team (Appendix 6).

Further information and advice regarding cyber bullying can be found in the DfE guidance documents:
Preventing and Tacking Bullying 2017
Cyberbullying: Advice for Head Teachers and School Staff 2014.

https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Pupil-Friendly Online Safety Policy

Chapel Allerton Primary School's School Council have created a pupil-friendly online safety policy which we proudly share with our school community. The policy can be viewed via the link below:
Childrens Policies | Chapel Allerton Primary School

Review of Policy

There are on-going opportunities for staff, children and families to discuss online safety concerns with the staff in school. This policy needs to be reviewed every 12 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted, or any guidance or orders are updated.

Appendix

1. Pupil Acceptable Use of Computing Agreement/Online Safety Rules
2. Staff, Student, Volunteer, Governor and Visitor Acceptable Use Agreement
3. Parent/carer and pupil Acceptable Use Agreement
4. Flow chart for managing an online safety incident not involving any illegal activity
5. Flow chart for managing an online safety incident involving illegal activity
6. Advice for children, parents and carers on Cyber bullying
7. Online Safety questionnaire KS1
8. Online Safety questionnaire KS2
9. Parent/guardian image consent form

Appendix 1

CHAPEL ALLERTON PRIMARY SCHOOL

Pupil Acceptable Use of Computing Agreement/Online Safety Rules

- I will only use computing in school for school purposes.
- I will only use my Purple Mash e-mail address when e-mailing in school.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my computing passwords to keep my personal information safe.
- I will only open/delete my own files.
- I will not bring software, CDs or computing equipment into school without permission

(unless my teacher tells me to).
• I will only use the Internet after being given permission from a teacher.
• I will make sure that all computing contact with other children and adults is responsible, polite, respectful 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 to any contact online unless a teacher, parent or carer has consented this.
• 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 computing because I know that these rules are to keep me safe.
• I know that the school may check my use of computing 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 online safety.

Appendix 2

Chapel Allerton Primary School Computing Acceptable Use Agreement for Staff, Students,

Volunteers, Governors & Visitors

Overview

The main points of this agreement can be summarised in the key sentences below.
Users are **NOT permitted** to undertake any of the following actions:

1. Logging on to the network with another user's account
2. Using computers to send offensive or harassing material to others, either internal or external to the school.
3. Altering the settings of the computers or making other changes which render them unusable by others
4. Physically tampering with equipment
5. Attempting to access unauthorised areas of the network
6. Accessing inappropriate web sites or trying to circumvent the school's systems. This includes the use of proxy servers or VPNs.
7. Attempting to spread viruses via the network
8. Using school computers for any form of illegal activity, including software and music piracy.

Breach of the acceptable use agreement may result in disciplinary action being taken.

For the purpose of this document, any electronic, mobile, computing device (for example laptop, netbook, tablet, and mobile phone) will be referred to as a mobile device.

Computer Facilities

Rules

The following rules apply to all computers which are provided by the school or connected to the school network.

General Conduct and Use

Any damage to equipment should be reported to ICT. The same applies to any apparent malfunction of equipment.

Use of the School Network

1. When logging on to the network, staff must always use their own user username and password.
2. Any member of staff who identifies a security problem on the School network must notify ICT immediately.
3. Staff must never divulge their passwords or write them down unless required to do so by ICT for support purposes. Any member of staff who suspects that their password has been compromised, accidentally or otherwise, should change their password without delay and report this potential security breach to ICT.
4. Staff must not use the network to gain unauthorized access to any other computer network.
5. Staff must not attempt to spread computer viruses; any infections must be reported immediately.
6. Staff must understand that the information they hold on the network is not private.
7. Staff must not store personal documents/pictures/music on their school documents areas (X drive or Shared Area). Any files meeting this description may be removed without prior notice.
8. Before leaving a computer unattended, staff must always log off or lock their workstation and check that this procedure is completed.

Monitoring

Staff accept that their computer, internet, email usage and printing may be monitored for the purpose of support, safety and security. Anything that is found to contravene any of Chapel Allerton Primary Schools Policies will be reported to the relevant person and the required action will be taken.

Data Protection

Data protection is the responsibility of all members of staff.

1. Staff must not disclose to a third party the personal details of another member of staff, a pupil or a pupil's family. When sending emails, staff should ensure the anonymity of addressees by making use of the BCC (blind carbon copy) functionality when addressing emails.
2. Staff must ensure that they do not retain copies of the personal details of another member of staff, a pupil or a pupil's family on their devices. Data of this type can be accessed via SIMS, therefore, paper copies of lists and/or other pupil data must not be taken home.
3. Staff must ensure that devices connected to school accounts are kept secure whilst in and out of school and report any loss to ICT immediately.

4. Staff must not store school data on any third party cloud servers, unencrypted USB sticks or external hard drives.

5. Do not disclose sensitive information to third parties without authorisation from the relevant Manager.

6. Staff should also refer to the School Data Protection Policy.

Child Protection

Staff are reminded that The Protection of Children Act 1978 prohibits at Section 1(1)(a) the "taking or making" of an indecent photograph or pseudo-photograph of a child.

According to the Memorandum of Understanding between Crown Prosecution (CPS) and Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003:
"Making includes the situation where a person downloads an image from the internet, or otherwise creates an electronic copy of a file containing such a photograph or pseudo-photograph. To be an offence such "making" must be a deliberate and intentional act, with the knowledge that the image made was, or was likely to be, an indecent photograph or pseudo-photograph of a child"

Internet and E-mail

Internet

Whilst the school internet facilities exist principally for enhancing the educational purposes of the school, staff may make personal use of the internet in their own time provided this doesn't detrimentally affect the school's primary function. Staff should also be aware that all internet usage is logged.

1. Staff must not breach another person's copyright in any material.

2. Staff must not attempt to access inappropriate websites using the school network and should be aware that all websites accessed are logged.

3. Staff must not upload or download any unauthorised software or attempt to run that software. In particular hacking, encryption and other system tools are expressly forbidden.

4. Staff must not engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden.

Email

1. Staff must not send electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable.

2. Staff must not make inappropriate use of the email system and address book, such as sending bulk emails, chain emails or for personal marketing purposes.

3. Staff must not use their email account to send or exchange material of an undesirable or illegal nature.

4. School email accounts should only be used for school related purposes. Personal emails and mailing lists from sources not relating to school may be blocked without notice.

5. Sensitive school information must not be forwarded to any personal email accounts.

6. Staff are permitted to configure Schools issued Email accounts for use on personal devices and computers provided that the device is Password or Pin code protected and had regularly updated software antivirus installed.

Online Collaboration and Storage Resources

SharePoint and OneDrive

Online resources such as SharePoint are to be treated in the same respect as onsite resources

1. When logging on to SharePoint or OneDrive, staff must always use their own user username and password.
2. Any member of staff who identifies a security problem must notify ICT immediately.
3. Staff must never divulge their passwords or write them down unless required to do so by ICT for support purposes. Any member of staff who suspects that their password has been compromised, accidentally or otherwise, should change their password without delay and report this potential security breach to ICT.
4. Staff must not attempt to spread computer viruses; any infections must be reported immediately.
5. Staff must understand that the information they hold on the network is not private to the individual.
6. Staff must not store personal documents/pictures/music on SharePoint or OneDrive. Any files meeting this description may be removed without prior notice.

Using Email and Online Resources on Personal Devices

Staff Are Permitted to Configure and use email and SharePoint for use on personal devices such as phones mobile devices and home computers provided the following rules are followed

1. Access to online resources are strictly to be used by the authorised staff member and not by any other member of the household. Devices must never be left unlocked and unattended at any time.
2. Appropriate security measure must be in place to prevent unauthorised access such a user passwords and pin numbers.
3. Antivirus software must be installed and update regularly on any home computers in order to provide adequate security.

Software

1. All Chapel Allerton Primary School installed software is subject to change and may be updated or removed at the school's discretion when deemed necessary.

2. Staff should not attempt to alter or remove any software installed on school computers without consultation with ICT.

Laptops & Mobile Devices

Where Required Staff are provided with either a laptop or mobile device to better aid ability and performance of their teaching and/or administrative duties.
School Issues laptops & mobile devices will be fully supported and maintained by ICT.
By accepting the provision of a laptop/mobile device, staff agree to the above policy and in addition the following rules:

Rules

Connection to the network

1. In order to help keep the network secure, safe and virus free, connection to the Chapel Allerton Primary School network of any unauthorised device is strictly forbidden. The only devices that can connect to the Chapel Allerton Primary School network are those which have been authorised by ICT.

2. School laptops should be connected to the school network at least once a week to ensure that any necessary windows/software/antivirus updates can take place.

3. Under no circumstances should any school equipment be removed from the network to make way for a laptop/mobile device.

Damage or loss

1. The school cannot accept responsibility for any damage caused to laptops or their contents (files, folders etc.) by inappropriate use.

2. It is the Users responsibility to backup any Data that is not stored in the Users documents areas (X drive) as this exists solely on the device and is not synchronised with the School Servers.

3. Any damage to laptops or mobile devices, whether accidental or otherwise, should be reported to ICT as soon as possible. A charge may be incurred if a school owned laptop/device is damaged by improper use. A charge may also be incurred to cover insurance excess if the laptop/device is lost or stolen due to insufficient security.

4. Whilst in transit, laptops/devices must be stored out of site, preferably in the boot of the car. If the car is left unattended then the laptop/device MUST be stored in the boot, out of site. Failure to do so will negate the school insurance cover and the member of staff may be liable for the cost of a replacement.

5. At home, laptops/devices must also be stored out of site, preferably in a locked draw or cupboard, when not in use.

Working at Home/Personal Use

4. Staff are permitted to use Laptops/Devices for light personal use provided that it does not hinder its School use. Any related personal data but not be excessive and must comply with Copyright, Child protection and Data Protection regulations.

5. Laptops/devices are to be used at home strictly by the authorised staff member and not by any other member of the household. Devices must never be left unlocked and unattended at any time. Any data that is stored on any laptop/device that appears to from other users will be deleted without prior notice.

Licensing and copyright

1. Staff are permitted to install limited software on School issued laptops provided that you have prior consent from ICT. It is the responsibility of the staff member to obtain valid licences for any software installed other than that already provided with the laptop/device. The Staff Member must also ensure that the software is free from viruses, malware and adware. Any software found to be in breach of these terms or identified as a possible cause to inflict adverse effect on the network or other devices will be removed without notice.
   Failure to comply with this will result in installation rights being revoked.

2. Staff are responsible for ensuring that the copyright of media files (music, images and video) is not breached by illegal copying of such files.

3. Staff are responsible for the material that exists on or is accessed via their laptop/device.

Printing & Copying

1. Staff must not print/copy any personal documents or pictures without reason or consent.

2. Staff must always log on to the copier using their own user PIN number.

3. Staff must never divulge their PIN number or write them down unless required to do so by ICT for support purposes. Any member of staff who suspects that their PIN number has been compromised, accidentally or otherwise, should change it without delay.

Social Media

When using personal social media:

1. Staff are solely responsible for any content on their own personal social media networks and electronic devices.
2. Staff are responsible for managing their own applications and content to ensure that it does not breach the school's safer working practice guidance or undermine public confidence in the school or the education profession.
3. Staff are personally responsible for security and privacy settings when using social media via their chosen equipment.
4. Staff are responsible for ensuring their own use of ICT and social media is professional and appropriate at all times.
5. Staff must not establish or seek to establish social contact with students, for the purpose of securing a friendship or to pursue or strengthen a relationship.
6. All contact with students should be through appropriate channels at all times and should be within clear and explicit professional boundaries.

User Signature:

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

Full Name ……..... (printed)

Job title: ……

Signature ……..…….…… Date ……

Appendix 3

CHAPEL ALLERTON PRIMARY SCHOOL

Acceptable use of computing agreement

Dear Parents/Carers,

Computing, including the internet, e-mail and mobile technologies, has become a growing and important part of learning in school. We expect all children to be safe and responsible when using any computing in school and to continue this at home.

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 computing Agreement is a summary of our E-Safety Policy which is available in full on our website or as a hard copy in our Office/Reception.

Yours sincerely,

Nicholas Sykes

Headteacher

……

Pupil Name: _____ **Class:** _____

I have read, understood and agreed with the Rules for Acceptable use of computing.

Signed …… (child)

Parent's/Carer's Consent for Internet Access:

- I have read and understood the school rules for Acceptable Use of computing and give permission for my child 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 to support my child to safely access the internet/computer etc at home to complete any necessary school tasks/homework. I will take all reasonable precautions to ensure they cannot access inappropriate materials and that they will use the computer in an appropriate manner.

Signed……..…… (parent/carer) Date……

Appendix 4

Managing an e-safety incident *not involving* *any illegal activity*

Commented [MW5]: Obviously this might be worth doing in the future as we are only wanting to get up to date now - but creating more of a visual flowchart might be easier - as we could distribute these to staff yearly? Or have them up somewhere

Incidents not involving any illegal activity, such as:
- using another person's username 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)

All e-safety concerns should be logged on CPOMS and kept as evidence. Staff should:

[] record electronically the incident and contact the head teacher about the incident

[] keep any evidence.

Did the incident involve a member of staff?

If the member of staff has:

1. behaved in a way that has or may have harmed a child.

2. possibly committed a criminal offence

3. behaved in a way which indicates s/he is unsuitable to work with children.

The head teacher would be notified and appropriate action would be taken after:

 review evidence and determine whether incident is accidental or deliberate

 decide upon the appropriate course of action

 follow school disciplinary procedures.

Did the incident involve a child?

Pupil as victim
In-school action to support pupil by one or more of the following:
 Class teacher
 Head teacher
 Designated person for Child Protection.
Inform parents/carer as appropriate
If the child is at risk contact the relevant outside agency.

Pupil as investigator
 Review incident and identify if other pupils were involved.
 Decide appropriate sanctions based on school rules.
 Inform parents/carers if serious or persistent incident.
 In serious incident contact the relevant agency as the child as instigator could be at risk.
 Review school procedure/policy to develop best practice.

Appendix 5

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

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

Was illegal material or activity found or suspected?

Yes
1. Inform the police and follow any advice given by the police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account
3. Save ALL evidence but DO NOT view or copy. Let the police review the evidence
 If a pupil is involved contact the Child Protection School Liaison Officer.
 If a member of staff is involved contact the relevant outside agency

No
If the incident did not involve any illegal activity refer to flowchart relating to non-illegal incidents.

Appendix 6

Advice for children and parents on Cyber-bullying and e-safety

Advice for parents/carers

• **Childnet** offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support.
• **Commonsensemedia** provide independent reviews, age ratings, & other information about all types of media for children and their parents.

• **Internet Matters** provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world.

• **Let's Talk About It** provides advice for parents and carers to keep children safe from online radicalisation.

• **London Grid for Learning** provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

• **Lucy Faithfull Foundation StopItNow** resource can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online).

• **National Crime Agency/CEOP Thinkuknow** provides support for parents and carers to keep their children safe online.

• **Net-aware** provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games.

• **Parentzone** provides help for parents and carers on how to keep their children safe online.

• **UK Safer Internet Centre** provide tips, advice, guides and other resources to help keep children safe online.

Advice for Children on Cyber-bullying

If you're being bullied by phone or on 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.
 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, carer or teacher as evidence.
 If possible, note the time and date bullying messages or images were sent and any details about the sender.

Support for children

• Childline for free and confidential advice

• UK Safer Internet Centre to report and remove harmful online content

• CEOP for advice on making a report about online abuse

Appendix 7

Anti-Bullying & Cyber bullying questionnaire KS1

Class……

Number of pupils taking part ……

1. What does e-safety mean?

2. What does the word cyber bullying mean?

3. If you saw something that worried you online who would you tell?

……

4. How many said they did not know who to tell?.....
5. How many children use the *internet* at home? ……
6. How many of those children use the internet;

    a. Alone……..

    b. With an adult……

7. What do you use the internet for at home?

…….

Appendix 8

Anti-Bullying & Cyber bullying KS2 Questionnaire

Name: _____ **Date:**_____

Class:_____

1. What do the words *Cyber bullying* mean?

2. If you felt that you were being bullied online, what would you do?

3. If you play games on the internet, do you play with people you do not know personally?

4. Do you know how to report rude or bullying messages online?

5. If saw something that worried you online, what would you do?