St Edmundsbury and Ipswich
Diocesan Multi Academy Trust

Hartest CE Primary School

Online Safety Policy

Prepared By	*Amanda Woolmer - Support Headteacher*
Approved by the Committee/Governing body	*LGB – Hartest CE Primary School*
Signature of Chair of Governors	Neil Gooding
Date Approved	*April 2020*
Review Date	*March 2022*

Online Safety Policy

Introduction

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of school/education setting or other establishments to ensure that children and young people are protected from potential harm both within and beyond the school/education setting or other establishment environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

This policy has been updated to include Online Safety Advice for parents during the Covid-19 period where children are working at home.

This policy should be read in conjunction with the schools policies for Safeguarding, Anti-Radicalisation, Whistleblowing and Acceptable Use of ICT.

Aims

This policy aims to explain how staff members, parents/carers or children can be a part of these safeguarding procedures. It also details how children are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'online safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Roles and Responsibilities of the School

It is the responsibility of all staff members to know who the Designated Safeguarding Lead Person is and to record and report any safeguarding concerns relating to online safety according to the school's safeguarding procedures (see Safeguarding Policy).

Governors and Designated Safeguarding Lead

At Hartest CE Primary School, the Designated Safeguarding Lead (DSL) is the Headteacher (see Safeguarding Policy). It is the overall responsibility of the DSL with the Governors to ensure that there is an overview of online safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The DSL is designated as the Online Safety Lead, supported by the Computing Subject Leader, to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring online safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who takes this role within the school.
- The DSL and the Governing Body ensure that there is a disclaimer on e-mails stating that the views expressed are not necessarily those of the school or the MAT (on the main school email address).
- Time and resources should be provided for the Online Safety Lead and staff to be trained and update policies, where appropriate.

- The DSL is responsible for promoting online safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The DSL should keep Governors informed of online safety developments and ensure Governors understand the link to safeguarding.
- The Governors **MUST** ensure online safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded. There is a recommended checklist for this purpose (see Appendix 3).
- An Online Safety Governor (Safeguarding Governor) challenges the school about having an Acceptable Use Policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:

  Challenging the school about having:

    - Firewalls.
    - Anti-virus and anti-spyware software.
    - Filters.
    - Using an accredited ISP (internet Service Provider).
    - Awareness of wireless technology issues.
    - A clear policy on using personal devices.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, (see the Managing Allegations Procedure on Suffolk Local Safeguarding Children's Board website) and appropriate action is taken.

Local Online Safety Lead (DSL) and Computing Subject Leader

It is the role of the DSL, alongside the Computing subject leader, to:

- Appreciate the importance of online safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Raise awareness and maintain a safe ICT learning environment within the school e.g. by displaying online safety posters and sending home leaflets.
- Keep parents informed of online safety issues e.g. by organising workshops / adult learning opportunities and sending home leaflets.
- Ensure that the Acceptable Use Policy is reviewed annually, with up-to-date information and that staff members and parents feel informed and know where to go for advice.
- Ensure that anti-virus software and anti-spyware is sufficient and up-to-date and that filtering is set to the correct level for staff, children and young people.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Ensure staff are familiar with changing technologies and how they are used and accessed, including use of apps, tablets and other 'smart' devices, including wearable technologies.
- Report serious concerns to the Governing Body. Technical issues should be reported to the LGB if there are cost implications. Safeguarding concerns should be reported to the Safeguarding Governor and the LGB.
- Liaise with the PSHE, Safeguarding and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Remind staff about the Acceptable Use Policy and monitor whether it is being adhered to. Any minor irregularities, such as unauthorised software, will be reported to the member of staff to rectify. Serious breaches will be reported to the Governors.
- Record safeguarding incidents or risks (see Safeguarding Policy).

- Alert staff to the issue of viruses being transmitted via new programmes and memory sticks and remind them to take care when transferring data.
- Remind staff to beware of unsolicited e-mails from other sources. Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.

Staff or Adults

It is the responsibility of all adults within the school to:

- Be familiar with the Safeguarding, Whistleblowing, Behaviour, Anti-Bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the DSL immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Be familiar with and adhere to the Acceptable Use of ICT and Mobile Phones Policy.
- Report any safeguarding concerns to the DSL, following the Safeguarding Policy. Report technical concerns e.g. about filtering levels to the ICT Subject Leader / ICT Technician.
- Report accidental access to inappropriate materials to the DSL and ICT Subject Leader in order that inappropriate sites are added to the restricted list or access can be controlled.
- Alert the DSL of any new or arising issues and risks that may need to be included within policies and procedures.
- Raise children’s awareness of online safety so that they can use technology in a safe way. Children should know what to do in the event of an incident.
- Be up-to-date with online safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Be familiar with changing technologies and how they are used and accessed, including use of apps, tablets and other ‘smart’ devices.
- Report incidents of personally directed ‘bullying’ or other inappropriate behaviour via the Internet or other technologies using the accident/incident reporting procedure in the same way as for other non-physical assaults.
- Check searches and websites prior to lessons so that the chance of children seeing inappropriate material is minimised.

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should receive a copy of the Acceptable Use of ICT Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school/education setting or other establishment, to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use. When accessing the Learning Platform from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

Children

Children should be:

- Responsible for following the Acceptable Use Policy for Children (Appendix 2) whilst within Hartest CE Primary School as agreed at the beginning of each academic year or whenever a new child attends the school for the first time.
- Taught to use the internet in a safe and responsible manner through Computing, PSHE or other clubs and groups.
- Responsible for following instructions and rules that are designed to keep them safe when using technology. Children in Key Stage 2 are asked to sign an Acceptable Use Policy for Children (Appendix 2) as part of the school's efforts to raise awareness.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

In the Event of Inappropriate Use by Children

The Acceptable Use Policy for Children (Appendix 2) details how children are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

Hartest CE Primary School encourages parents/carers to support the agreement with their child. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school.

Should a child be found to misuse the online facilities whilst at school, the following consequences should occur.

- ○ Any child found to be misusing the internet by not following the Acceptable Use Policy for Children may be suspended from using the internet for a particular lesson or activity.
- ○ Further misuse of the agreement may result in not being allowed to access the internet for a period of time and parents/carers may be informed.
- ○ A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window so that an adult can take the appropriate action. Where a child feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

The Curriculum and Tools for Learning

Internet Use

Children are taught how to use the Internet safely and responsibly. They should also be taught, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave *Year 6*:

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

Children should be made aware of personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School/education setting or other establishment.
- Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school.
- Identifying information, e.g. I am number 8 in the school Football Team.

Children should be supervised and monitored when they have access to the internet during school time. The management of internet use and the risks associated with this should be considered by teachers when planning lessons.

Pupils with Additional Learning Needs

The school should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

School Website

At the beginning of each year the school seeks the permission of parents for photographs to be taken of children and for those images to be used in appropriate public places, such as newsletters, brochures and on the school website. Photographs are not published alongside the names of children.

External Websites

In the event that a member of staff or child finds themselves or another person on an external website e.g. as a victim of cyber-bullying, he / she is encouraged to report this to the DSL and any other appropriate authority depending upon the nature of the incident.

E-mail Use

The school may have e-mail addresses for children to use, as a class and or as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms. Email may be used to correspond with children from other schools or countries and can be used to enhance the curriculum in many ways. Teachers are expected to monitor class use of emails where there are communications during school time.

Children should use school issued email addresses for approved communication only e.g. with a 'pen pal' from a partner school. A breach of this may be considered a misuse.

Parents/carers are encouraged to be involved with the monitoring of emails sent from home, understanding who their child is communicating with and for what purpose, assessing risks together.

Mobile Phones, Smart Devices & Other Emerging Technologies

Increasing numbers of children have access to mobile phones and other 'smart' technologies and may bring them to school. When children bring Mobile Phones or other Smart Technologies into school they should be taken to the School Office and left in the safe until 'home' time. The use of mobile technologies can be used as a teaching and learning tool within the curriculum. The following areas of concern must be considered:

- Inappropriate or bullying text messages.
- Images or video taken of adults or peers without permission being sought.
- 'Happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed.
- 'Trolling' – the defaming of another person's character through persistent dialogue, gossip, spreading rumours or inciting argument
- 'Sexting' - the sending of suggestive or sexually explicit personal images via mobile phones.
- Wireless Internet access, which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.
- The safeguarding risks relating to contact between children and staff members using smart technologies.

Personal Mobile Devices

Staff should be allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- Staff should be aware that games consoles such as the Sony PlayStation, Microsoft Xbox and other such systems have Internet access which may not include filtering. Before use within school/education setting or other establishment, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.

- The school/education setting or other establishment is not responsible for any theft, loss or damage of any personal mobile device.

Video and Photographs

The term ‘image’ refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in school, children have access to a variety of visual and sound recording equipment.

The sharing of photographs via weblogs, social media or any other means online should only occur after permission has been given by a parent/carer or member of staff.

Photographs/images used to identify children and young people in a forum or using Instant Messaging within the learning platform should be representative of the child rather than of the child e.g. an avatar.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should not be presented alongside a child’s name for safeguarding reasons.

It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of children will only be used after permission has been given by a parent/carer.

Managing Social Networking and Other Web 2.0 Technologies

Social networking sites, such as Facebook, Instagram and WhatsApp, have emerged in recent years as a leading method of communication, proving increasingly popular amongst both adults and young people alike. The service offers users both a public and private space through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed.

With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published.

In response to this issue the following measures are in place:

- The school should control access to social networking sites during the school day.
- Children are advised against giving out personal details or information.
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse.
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to ‘Friends only’ for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The school should be aware that social networking can be a vehicle for cyber-bullying. Pupils are encouraged to report any incidents of bullying to the school allowing for the procedures, as set out in the anti-bullying policy, to be followed.

Social Networking Advice for Staff

Social networking outside of work hours, on non-school/education setting or other establishment-issue equipment, is the personal choice of all school/education setting or other establishment staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils or parents, such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent pupils or parents from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with pupils outside of Headteacher authorised systems (e.g. school/education setting or other establishment email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent pupils or parents from accessing photo albums or personal information.

Links to Other Policies - Behaviour and Anti-Bullying Policies

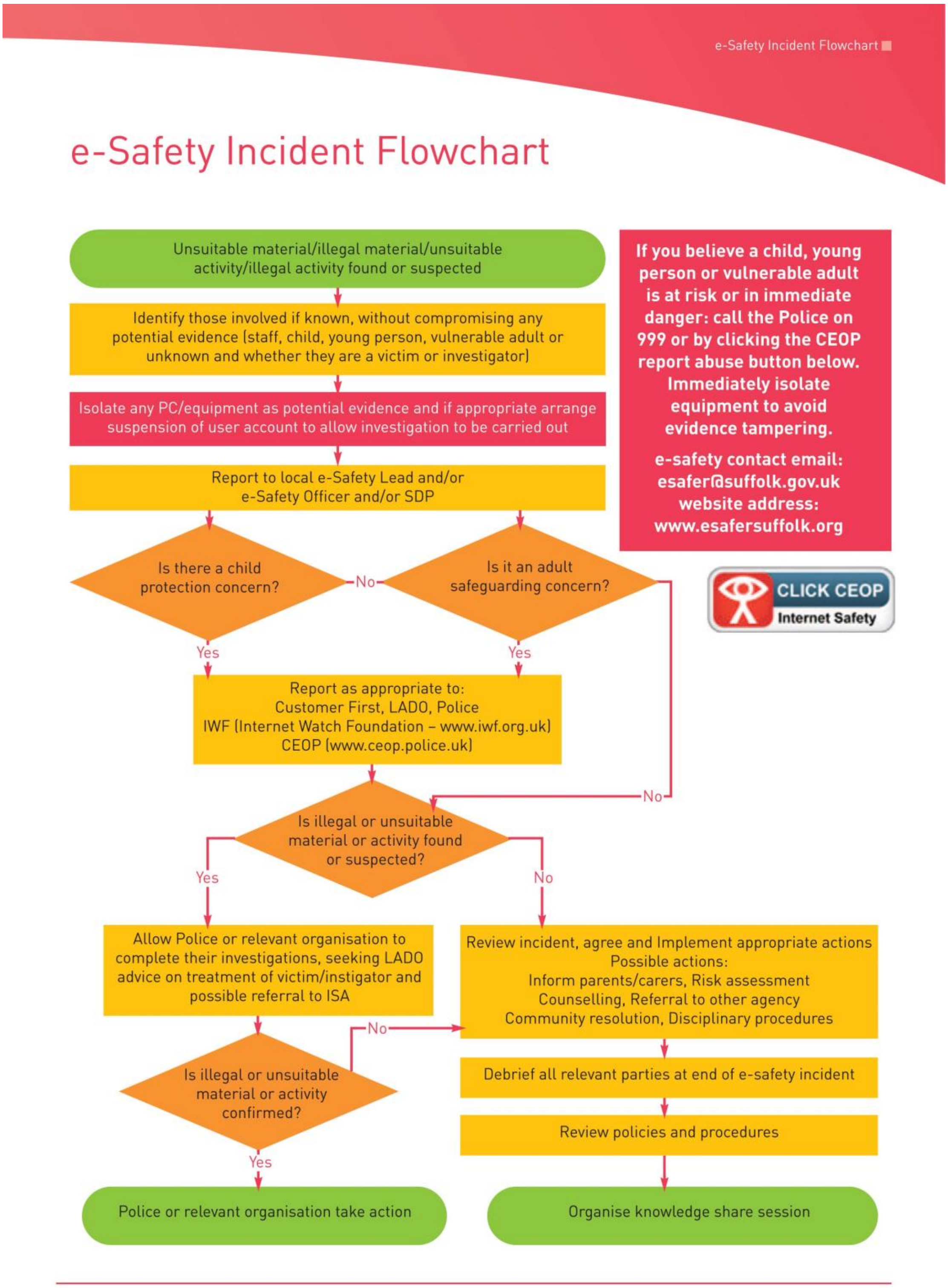
Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs. The school has an Anti-bullying Policy, which refers to cyber-bullying issues.

All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all ICT and PSHE materials for children and their parents/carers. People should not treat online behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour. This is a key message which is reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour.

Allegations of misuse against members of staff should be dealt with according to the Safeguarding Policy. This may involve referring the incident to the Local Authority designated Officer (LADO) without internal investigation.

Appendix 1

Online Safety Flow Chart



e-Safety Incident Flowchart

e-Safety Incident Flowchart

Unsuitable material/illegal material/unsuitable activity/illegal activity found or suspected

Identify those involved if known, without compromising any potential evidence (staff, child, young person, vulnerable adult or unknown and whether they are a victim or investigator)

Isolate any PC/equipment as potential evidence and if appropriate arrange suspension of user account to allow investigation to be carried out

Report to local e-Safety Lead and/or e-Safety Officer and/or SDP

Is there a child protection concern?

No

Is it an adult safeguarding concern?

Yes

Yes

Report as appropriate to:
Customer First, LADO, Police
IWF (Internet Watch Foundation – www.iwf.org.uk)
CEOP (www.ceop.police.uk)

No

Is illegal or unsuitable material or activity found or suspected?

Yes

No

Allow Police or relevant organisation to complete their investigations, seeking LADO advice on treatment of victim/instigator and possible referral to ISA

Review incident, agree and Implement appropriate actions
Possible actions:
Inform parents/carers, Risk assessment
Counselling, Referral to other agency
Community resolution, Disciplinary procedures

No

Is illegal or unsuitable material or activity confirmed?

Debrief all relevant parties at end of e-safety incident

Review policies and procedures

Yes

Police or relevant organisation take action

Organise knowledge share session

If you believe a child, young person or vulnerable adult is at risk or in immediate danger: call the Police on 999 or by clicking the CEOP report abuse button below. Immediately isolate equipment to avoid evidence tampering.

e-safety contact email: esafer@suffolk.gov.uk
website address: www.esafersuffolk.org

CLICK CEOP
Internet Safety

APPENDIX 2
ACCEPTABLE USE POLICY FOR CHILDREN

My Online Safety Agreement

This is my agreement for using the internet safely and responsibly.

- I will use the internet to help me learn.
- I will learn how to use the internet safely and responsibly.
- I will only send email messages that are polite and friendly.
- I will only email, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video conferencing.
- I agree never to give out passwords or personal information like my full name, address or phone numbers.
- I agree never to post photographs or video clips without permission or that I will not include my full name with photographs.
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to a trusted adult.
- If I see anything on the internet that makes me feel uncomfortable, I know what to do.
- If I receive a message sent by someone I don't know, I know what to do.
- I know I should follow these guidelines as part of the agreement with my parent/carer.
- I agree to look after myself and others by using my internet in a safe and responsible way.

Signed... Dated......................................

Appendix 3
Hartest CE Primary School
Acceptable Use Agreement for Staff, Governors and Visitors

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school/education setting or other establishment must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, e-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school/education setting or other establishment equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via e-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person’s safety to the Headteacher, DSL / Online Safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know who my DSL / Online Safety Lead is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use the school/education setting or other establishment e-mail address and phones (if provided) and only to a child’s school/education setting or other establishment e-mail address upon agreed use within the school/education setting or other establishment.
- I know that I must not use the school/education setting or other establishment system for personal use unless this has been agreed by the Headteacher or DSL / Online Safety Lead.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Online Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school/education setting or other establishment filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of Online Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed………………………………………………….Date…………………….

Name (printed)……………………………………………………

Appendix 4

E-safety Checklist for Schools

ZIP IT BLOCK IT FLAG IT

CLICK CLEVER CLICK SAFE

Policies, practice and monitoring	**Yes**	**No**	**Action**
Does the school have an e-safety policy in place?			
Are there 'Acceptable Use Policies' for both pupils and adults?			
Is cyber bullying addressed in the school's anti-bullying policy?			
Are there effective sanctions in place for breaching the policy?			
Has the school appointed an e-safety lead?			
Is e-safety provision rigorously and regularly reviewed?			
Does the school keep a log of e-safety incidents and alter provision accordingly?			
Has an evaluative comment on e-safety been included in the Safeguarding self-review assessment?			
Infrastructure	**Yes**	**No**	**Action**
Is the school network safe and secure?			
Does the school use an accredited internet service provider? *Eg E2BN*			
Does the school use internet filtering/monitoring?			

If there are changes made to the internet filtering setup are these authorised by a senior manager?			

Learners	Yes	No	Action
Do learners understand what safe and responsible online behaviour means and do they use it?			
Is e-safety education a regular part of the curriculum?			
Do learners know and understand the UKCCIS digital code –			
Do learners know how to report e-safety concerns they may have? *Eg CEOP Report Abuse button, reporting to an adult in school*			

Staff	Yes	No	Action
Do teaching staff understand e-safety issues and risks?			
Have they received training which is regularly updated?			
Do staff know who to report to with an issue of concern regarding e-safety?			
Do they keep data safe and secure? Eg personal assessment data, use of password protected files			
Do they take measures to protect themselves online? *Eg keep personal information private, use secure passwords*			
Do they conduct themselves professionally online? *Eg social networking sites, blogs*			

Parents / Governors	Yes	No	Action
Do governors have a general understanding of the issues and risks associated with e-safety?			
Does the school keep parents aware of e-safety issues through eg newsletters, leaflets, open assemblies, updates etc?			
Has the school held an e-safety Parent Awareness Session?			

APPENDIX 5

Online Safety during COVID 19

As you will all be aware, Hartest CE Primary School will be partially closed from Friday 20th March in response to the current situation with coronavirus (COVID-19).

We are aware that this is likely to mean that many children will be spending an increased amount of time online over the coming weeks. Online safety is an important part of keeping children safe at Hartest CE Primary School and as such we would like to share some helpful advice to help you consider how you can keep your family safer online at home.

Follow the GOLDen Rules

Ground Rules

- Discuss and agree as a family how the internet will be used in your house at a level that is appropriate to your children's ability and age.
- Discuss with your children what they think is and isn't acceptable to do online, then add your own rules and boundaries to the list.
- Decide on what information should be kept private online, such as contact information, photos in school uniform, and agree rules for making and meeting online friends.
- Set clear boundaries relating to use of webcams, video chat, live streaming and live voice on different devices; even when children are talking to people they already know, they can still experience risks. Find more information about live streaming at: www.thinkuknow.co.uk/parents/articles/live-streaming-responding-to-the-risks/
- Explore how to create strong passwords and discuss how to keep passwords safe, for example not sharing them with their friends or using the same password for several accounts.
- You might find it helpful to write 'grounds rules' down as a visual reminder. See a template 'family agreement' at: www.childnet.com/resources/family-agreement
- Remember these are whole family rules, so consider your own use of the internet and lead by example. Think about how much time you spend online and consider the information you are sharing on your social networks about your children and who can see it.
- Share quality time together. Consider nominating 'tech-free' areas or times, such as your child's bedroom or dinner time, where you can give each other undivided attention and share offline experiences, like reading a book together.

Online Safety

- Install antivirus software and secure your internet connection.
- More advice on online security can be accessed at www.getsafeonline.org/
- Make the most of the parental controls on your children's internet enabled devices and games consoles to help restrict access to inappropriate content. They can also help you manage how much time your child spends online.
- Do your research and select the tools which are most suitable to you, your child and the technology in your home. Find more information on parental controls at:
- www.internetmatters.org
- www.saferinternet.org.uk/advice-and-resources/a-parents-guide
- Set up filters on internet search engines to limit the likelihood of your children accidentally coming across inappropriate content when searching online.
- Ensure your child understands that parental controls are in place to protect them, not restrict them; some children will actively work around parental controls if they feel constrained without knowing why.
- Read any parental guidance and safety recommendations for games, apps or websites **before** allowing your child to use them.
- The following guides provide balanced information to help you make informed decisions:
  - www.net-aware.org.uk,
  - www.askaboutgames.com/
  - www.commonsensemedia.org

- Be aware that parental control tools and filters are not always 100% effective and you can't rely on them alone to protect your child online. It's important to monitor and supervise your child's online activities; where possible access should take place in a family area, but this will depend on the age and ability of your child.

Learning

- The internet provides vast opportunities for children, both educationally and socially, especially during the current situation. As adults, it is important that we acknowledge the many wonderful and positive opportunities the internet provides for our children; we just need to steer them in the right direction.
- ○ Ensure you make appropriate checks on anyone online offering educational support to you and your child; whilst many people will be acting with good intentions, it's important that we are all vigilant when children are using the internet and act together to ensure they are protected from anyone who may pose a risk to them.
- ○ Encourage your child's creativity by teaching them how to take photos or make videos safely; these can be used to make a collage or be shared with family and friends.
- ○ Being online should be a sociable activity; keep your devices in a communal area and take it in turns to choose a game or video that the whole family can enjoy together. Why not take it in turns the good old fashioned way to beat the highest scorer?!
- ○ Create learning opportunities; just because they're not at school, doesn't mean children can't continue to learn new things. There are a number of educational apps and resources available online or simply encourage your children to safely research different things online.

Dialogue

- Maintain an open mind and positive attitude when talking with your child about the internet. Take an active interest in your child's online activities and engage in their online world with them.
- Ask your child which games, apps, websites or tools they like to use and why; playing together with your child can often open opportunities to discuss safe behaviour online.
- Ask your child if they know where to go for help; do they know where to find safety advice or information about privacy settings and know how to report or block users on their games and websites.
- Make sure your child knows that they should come to you, or another trusted adult, for help if something happens online that makes them feel scared, worried or uncomfortable.
- ○ Talk to your child about being kind online and encourage them not to retaliate or reply to cyberbullying and to keep any evidence; you may need to show your child how to take screenshots on their device.

- ○ Have a look at the following links for useful tips on talking to children about online safety in an age appropriate way:

- ○ www.childnet.com/parents-and-carers/have-a-conversation
- ○ www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/talking-your-child-staying-safe-online

Websites to visit for more information

Think U Know: www.thinkuknow.co.uk
The National Crimes Agency Child Exploitation and Online Protection Command (CEOP) have a website which is suitable for children aged 5-16 and a section just for parents/carers with advice and information.

NSPCC: www.net-aware.org.uk and www.nspcc.org.uk/onlinesafety
The NSPCC have produced resources for parents, including Net Aware, a tool which reviews some of the most popular apps. The website has helpful advice for parents about issues such as online grooming, 'sexting' and cyberbullying. They also provide a helpline for parents: 0808 8005002

ChildLine: www.childline.org.uk
The ChildLine website has a wide range of info and advice on both online and offline safety. There is info about online gaming, grooming which can be shared with children. They also provide a helpline for children: 0800 1111

UK Safer Internet Centre: www.saferinternet.org.uk
UK Safer Internet Centre provides a wide variety of advice and guidance to help you discuss online safety with your children. There are useful checklists for privacy settings on social networks and suggestions to consider before buying devices for your children.

Childnet: www.childnet.com
Childnet has resources, including videos and storybooks, to help you discuss online safety with your children. It includes advice on setting up parental controls, cyberbullying and setting up a family agreement for safer internet use.

Internet Matters: www.internetmatters.org
Internet Matters bring you all the information you need to keep your children safe online. It has a tool which guides you through how to set up parental controls on all the different devices in your home to protect your children.

Parent Info: www.parentinfo.org
Parent Info provides information to parents and carers about a wide range of subject matter, from difficult topics about sex, relationships and the internet or body image and peer pressure to broader parenting topics like 'how much sleep do teenagers need?'

BBC "Own It" Website and App: www.bbc.com/ownit and www.bbc.com/ownit/take-control/own-it-app
The BBC Own It Website aims to help children aged 8-13 "be the boss" of their online lives. The website has a range of videos and activities to explore with children and even has a helpful app which can be installed on children's devices to help them use technology responsibility

If you are worried

Be alert to any changes in behaviour, language and attitude in your child that may indicate that something is upsetting them online, for example, if your child starts to withdraw from family and friends or becomes secretive about their online behaviour.

If your child discloses an online issue or concern to you, ensure you **listen** to them.

- Avoid being angry or blaming them; reassure them that they have done the right thing by telling you.
- Take their concerns seriously; even if you feel they are overreacting or their worries are unfounded, it is important not to dismiss their feelings as this can prevent them from coming to you for help again in the future.
- Support your child to report and block people online who may have tried to contact them or have sent them nasty or inappropriate messages or content.
- Help your child to report to the site or service where the concern happened.

Depending on the issue, you can report specific concerns online at:

- Inappropriate content: https://reportharmfulcontent.com/
- Terrorist content: https://act.campaign.gov.uk/
- Child Sexual Abuse Imagery: https://www.iwf.org.uk/

- Online Child Sexual Abuse: https://ceop.police.uk/

The Designated Safeguarding Leads are available to discuss any help you may need or concerns that you may have.