Hopton CEVC Primary School

Online Policy &

Use of Social Networking sites

Approved by:

The Full Governing Body

The Governing Body of Hopton CEVC Primary School adopted this policy May 2017

Document change history:

Review date:	Reviewed & Approved by	Change details
December 2018	Craig Smith	Inserted statement (pg.4) outlining the responsibility for teaching staff to raise online concerns by following the outlined procedure on pg.9. Added to existing statement to include instruction to record online safety concerns on purple forms.
December 2019	Claire Wright	• Page 7: Use of SMART watches
December 2020	Claire Wright & FGB	• Page 2, point 1. Added section on remote learning • Page 5, point 10. Changed ICT to computing added a hyperlink to Jigsaw. • Page 5, point 11. Changed annual meetings to 'meetings' • Page 6 point 13, clarified phoned use. • Page 8, point 14, added the word 'laptops' • Page 9, point 1, added 'Live Stream Lessons for remote learning' • Page 10, point 18 added section for 'Remote Learning Platform' • Page 11, point 19, clarified phones use for ALL adults on site. • Page 13, added flowchart Hyperlink • Page 17, amended ACU to add Google Classroom • Page18, amended ACU to add Google Classroom
December 2021	Claire Wright & FGB	• Page 7: Update to the use of mobile phones for children • Page 11: Point 19 Clarify on the use of mobile phones for children. • Page 18, Mobile phones added • Page 18/19 Content, conduct and contact added to KS2 ACA • Appendix 1 added. Incident reporting form.
July 2022	Claire Wright	Updated after Online Safety Training • Page 3: Protection of staff by Head teacher • Page: 'Self Declaration'
November 2023	Claire Wright	CPW reviewed the policy for the school and suggested the following amendments: • Page 6: Section 12 Change of company name from Tecwyn to CPW Computing Ltd • Page 15: Section 4 Change of wording to use of 'use of social networking sites' • Page 6 & 7 Section 12: Added filtering section to **Managing ICT Systems and Access (Filtering & Monitoring)**
November 2024		

At Hopton CEVC Primary School we live out the words of Jesus in Matthew 19 vs 26 'With God all things are possible'. We raise aspirations and encourage perseverance to reach goals in life and learning.

Hopton CEVC Primary School Online Policy

1. Introduction

New technologies have become integral to the lives of children and young people in today's society. The internet and electronic communication allow teachers and pupils to learn from each other and access a wide range of information sources.

Digital and new technologies engage all pupils and allow teachers to develop an inclusive practice and enhance learning and teaching activities. Technologies enable pupils to access the wider curriculum and to present information in a wider variety of ways. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Pupils and all staff should have an entitlement to safe internet access at all times. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, pupils do not always have the knowledge, skills and understanding to keep them safe which can put them at risk inside and outside of the school. As schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).

Some of the potential dangers which they may face include

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/internet games.
- Inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the pupil.

Many of these risks reflect situations in the real/off-line world and this Online policy must be used in conjunction with other school policies e.g. Behaviour and Anti-bullying, Safeguarding and Child Protection, Curriculum Policies and the staff hand book. It is impossible to eliminate all risk and therefore essential to teach pupils to recognise potential dangers and to equip them with the skills to deal with them. Note – New concerns or risks can develop very quickly in the digital world and as such changes may be made to this policy before the review date.

As a school we must demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks.

The Online policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help pupils and their parents/carers to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Responsibilities of the school community

We believe that Online safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

3. Responsibilities of the Headteacher

- Develop and promote an online safety culture within the school community.
- Support the school online lead in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to online effectively.
- Receive and regularly review online incident logs and be aware of the procedure to be followed should an online incident occur in school.
- Take ultimate responsibility for the online safety of the school community.
- Protect the staff from being placed in vulnerable situations by ensure all lines of communication are clear.

4. Responsibilities of the Online lead

- Promote an awareness and commitment to online safety throughout the school.
- Be the first point of contact in school on all online safety matters.
- Create and maintain online policies and procedures.
- Develop an understanding of current online issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in online safety issues.
- Ensure that online safety education is embedded across the curriculum.
- Ensure that online safety is promoted to parents and carers.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on online safety issues to the rest of the staff and governors as appropriate.
- Ensure an online safety incident log is kept up-to-date.

5. Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's online policies and guidance.
- Read, understand and adhere to the school staff AUP (Acceptable Use policy).
- Develop and maintain an awareness of current online issues and guidance.
- Model safe and responsible behaviours in your own use of technology.

- Embed online messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an online incident occurs.
- Raise online safety concerns and disclosures to the designated Online Safety Lead following the protocol as outlined within this policy document.
- Maintain a professional level of conduct in their personal use of technology at all times. Please also refer to the social networking section of this policy (page 11)
- Deliver the online curriculum.
- Understand you can decline using your personal devise in school for your own protection and you have the right to say 'no' to the request (this relates to school trips and use of your personal phone)
- Ensure the Head teacher is made aware of any issues that arise, promoting the notion of 'self-declaration'.

6. Responsibilities of Technical Staff

- Read, understand, contribute to and help promote the school's online policies and guidance.
- Read, understand and adhere to the school staff AUP (Acceptable Use policy).
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school ICT system.
- Report any online related issues that come to your attention to the online safety lead.
- Develop and maintain an awareness of current online issues, legislation and guidance relevant to your work.
- Liaise with the local authority and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all
- times.

7. Responsibilities of Pupils

- Read, understand and adhere to the school pupil AUP (Acceptable Use policy).
- Help and support the school in creating online policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for your own and each others' safe and responsible use of
- technology in school and at home, including judging the risks posed by the personal
- technology owned and used by pupils outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in
- your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss online issues with family and friends in an open and honest way.

8. Responsibilities of Parents and Carers

- Help and support your school in promoting online safety.

- Read, understand and promote the school pupil AUP (Acceptable Use policy) with your children.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that your children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss online safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if you have any concerns about your children's use of
- technology.
- To be aware of the age restrictions on different apps.

9. Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's online policies and guidance.
- Develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviour in their use of technology in and out of school.
- Support the work of the online safety lead in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety activities.
- Ensure appropriate funding and resources are available for the school to implement their online strategy.

10. Teaching and Learning

We believe that the key to developing safe and responsible behaviour online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

We will provide a series of specific online safety related lessons in every year group as part of the Computing curriculum some of which will be reinforced through our RSE curriculum taught weekly and supported by the Jigsaw resources.

- We will celebrate and promote online safety through assemblies and whole-school activities.
- We will discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

11. How Parents and Carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Hold parents' meeting on online safety.
- Include useful links and advice on online safety in newsletters and on our school website

12. Managing ICT Systems and Access (Filtering & Monitoring).

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

- Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software are kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date by the ICT technician.
- All users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- At KS1 all internet access will be by working alongside a member of staff, or if working independently a member of staff will supervise at all times.
- At KS2 pupils' internet access will be supervised by a member of staff.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. head teacher and member of technical support.

Wireless networks to facilitate access to the school network and the internet are controlled and protected by CPW Computing Ltd so that unauthorised users nearby cannot inadvertently or deliberately connect.

Teaching staff and teaching assistants will be able to download information, documents, video clips, pictures and sound files that are copyright free, in line with their AUP (Acceptable Use policy) and filtered through the firewall.

Teaching staff, teaching assistants, admin and ICT technician are able to install updates, or relevant software for educational purposes or software for new digital equipment.

The ICT technician is able to change settings.

Teaching staff are able to use their own USB drives as long as they have been encrypted.

Images of pupils and staff must be stored on the shared school network and not on lap-tops or computers internal memory.

Pupils are able to download copyright free images and information for a specific educational purpose and in line with their AUP. They are not allowed to install, change settings or connect personal portable devices to school equipment.

Filtering

The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.

The school utilises the Cisco Meraki Firewall & Filtering solution. The filtering comes from an onsite firewall that protects any device linked to the schools' network without the need for additional configuration. It uses filter categories that are being maintained by identification by both Web and IP Reputation and Web Classification services. The sites identified in these filter categories are then blocked to prevent access to websites containing, for example, offensive materials (such as pornographic or violent imagery), distracting or time-wasting materials (such as social networking and non-educational games) and downloads of certain types of files (such as program or music files). The filter categories are constantly evolving and updates are automatically applied whenever a URL is requested

The school will regularly audit ICT use to establish if the online policy is adequate and that the implementation of the online policy and curriculum is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimise risks.

13. Learning Technologies in school

	Pupils	**Staff**
Personal mobile phones brought into school	Pupils not allowed in classrooms. Some parents require their children to travel to school with phones for safety reasons. These phones will be kept locked in the school office, for return at the end of the day.	Staff allowed
Mobile phones used in lessons	Pupils not allowed	Staff allowed in special circumstances with the permission of the HT (this would be for safety reasons when moving round or off the site)
Mobile phones used outside of lessons	Pupils not allowed	Staff allowed out of sight of pupils and parents
Taking photographs or videos on personal equipment	Pupils not allowed	Staff **not** allowed.
Taking photographs or videos on school devices (with school SD cards)	Pupils allowed at certain times Pupils allowed with permission	Staff allowed

Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	Pupils allowed at certain times Pupils allowed with permission Pupils allowed with supervision	Staff allowed at certain times
Use of personal email addresses in school	Pupils not allowed	Staff allowed at certain times
Use of school email address for personal correspondence	Pupils not allowed	Staff not allowed
Use of online chat rooms or polling sites	Pupils not allowed	Staff not allowed
Use of instant messaging services	Pupils not allowed	Staff not allowed
Use of blogs, wikis, podcasts or social networking sites	Pupils allowed at certain times Pupils allowed with permission Pupils allowed with supervision	Staff allowed at certain times (eg Posting upcoming events on the Hopton Facebook page) Staff may not use personal account on school equipment.
Use of video conferencing or other online video meetings	Pupils allowed at certain times Pupils allowed with permission Pupils allowed with supervision	Staff allowed at certain times
Use of a SMART watch	Pupils not allowed	Adults allowed for apps that will aid the classroom ie timer but not allowed to access personal communications.

14. Using Email

Staff, Governors and pupils should use school e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.

- Pupils are not permitted to access personal e-mail accounts during school.
- Staff should not access personal e-mail accounts on laptops during the school working day unless work-related.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately and evidence saved.

15. Using images, video and sound

We will remind pupils of safe and responsible behaviour when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

- Digital images, video and sound will only be created using equipment provided by the school or school staff.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.

16. Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

We may use blogs to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Blogging and other publishing of online content by pupils will take place within the school learning platform or website. Pupils will not be allowed to post or create content on sites where members of the public have access.
- Children and parents should not upload photos on social media sites or other forums such as Instagram wearing school uniform.
- Any public blogs run by staff on behalf of the school will be hosted on the learning platform or school website and postings should be approved by the Headteacher before publishing.
- Pupils will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them. Pupils will not use their real name when creating such resources. Through the online saftey curriculum they will be taught to create an appropriate 'nickname'.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviour in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

17. Live Stream Lessons for Remote Learning

- Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves. In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function.

- When planning the use of live stream platforms within remote learning our school will:

- Consider whether the technology is available to children/families and make alternative arrangements for provision where necessary.
- Ensure that staff are trained to use the technology.
- Ensure that children's behaviour/interactions are managed in line with the expectations of the school behaviour policy.
- Risk assess the platform being used and consider whether there are functions, such as live chat, pupil's use of video camera, or the recording of the session, which need to be disabled or which require further measures to support their appropriate use.

The above points are relevant to live stream in its broadest sense. What follows next is more relevant, but not exclusively, to the use of platforms allowing two-way video interaction between all users.

- Two members of staff will be 'within the room' when conducting a live stream session with pupils. If the session is being run from school and both adults are there, then they can be physically within the same room. If one or both adults are working remotely then this means that two adults will need to be present within the video call, and they should both be there before the pupils dial in.
- The second member of staff is there to provide a safeguard for both the pupils and the teacher, so does not need to be a curriculum specialist.
- The second member of staff could act additionally as technical/behaviour support, in terms of monitoring pupils' interactions and ensuring they are not using chat or recording features if these cannot be disabled.
- Sessions will be planned and scheduled for during school hours.
- Parents will be contacted to advise that the session is taking place and they and the child should consent to abide to an acceptable use agreement covering issues such as not recording the session, not using the live chat feature, being appropriately dressed etc.
- Only school devices and school contact numbers/emails will be used for communications and running the session.
- Only live streaming platforms approved by SLT will be used.
- Staff will dress professionally and choose a neutral background for their video stream.
- Pupils should be dressed appropriately e.g. clothes they might wear for a non-uniform day.
- Pupils should live stream from a suitable location within their household, not bedrooms.
- Staff behaviour and language will be entirely in line with the staff code of conduct.
- All other school policies/practices should be followed, notably the safeguarding and child protection policy so should there be any welfare concerns about the child these should be brought to the attention of the DSL without delay.

Live Stream from other providers

- When directing learners to any content from other providers, its suitability and appropriateness will be checked.
- Where that content may be live streamed, the safeguarding aspect of how that content is being delivered will be considered e.g. how children are able to interact, how is content and interactions being monitored/moderated etc?
- For one off live stream events, the content will be monitored by a member of staff along with the interactions/behaviour of the learners taking part.

- When/if multiple sessions are being run at various times during the school day, school leaders will check that they are satisfied with the safeguarding policy of the provider(s) and, then, monitor some sessions to check they are in accordance with the policy.

Using video calls for 1:1 sessions with children

- The school may consider using 1:1 video call sessions to support interventions with children such as mental health support or counselling.
- These sessions will only be provided where they have been risk assessed and approved by SLT.
- Where the communication with an individual child does not require the confidentiality of a counselling session, there will be two adults involved; this will provide a safeguard for the adults and the children.
- These two adults will either be physically in the same room, with the second member of staff being referenced to the child so that they are aware, or, where staff are working remotely, they will both be within the virtual room of the meeting.
- In either case both adults will be present before the child is admitted to the online session.

18.Remote Learning Platform

- Hopton School use Google Classroom to provide remote learning to the community when needed.
- Here children can find appropriate links and materials to their learning.
- Children and parents will respect the privacy of others by not sharing their access code to others outside of the school community.
- All children and adults will behave in line with the school's behaviour expectations on the site.
- Parents and carers will be mindful of the content that they post on the site, and monitor their own child's activity daily.
- Should there be any concern parents and carers should contact the school immediately.

19. Using mobile phones

- Pupils are not permitted mobile phones in classrooms. Those who travel to school with a phone for safety reasons will be asked to leave the phone in the school office.
- Where staff members are required to use a mobile phone for school duties, in case of emergency during off-site activities, they may use their personal mobile phones. All other times their phones should remain out of sight from the children
- Visitors and volunteers should not have their phones on them in school.

18. Using New Technologies

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an online safety point of view.
- We will regularly amend the online policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an online safety risk.
- To be mindful that emerging technologies are continuously developing and these will be reviewed and reflected in the online Policy.

19. Protecting Personal Data

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the Headteacher, and without ensuring such data is kept secure through an encrypted memory stick.

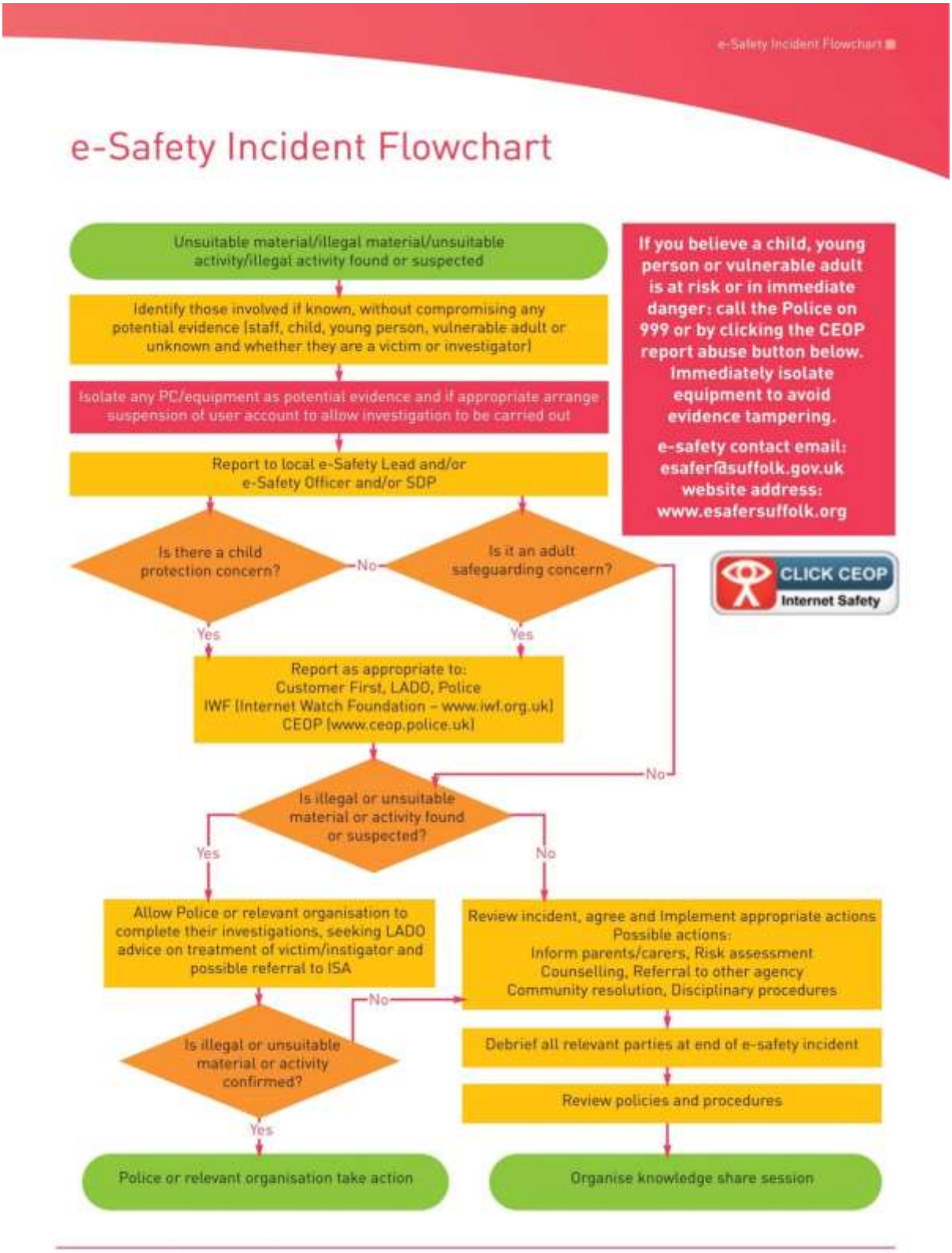
20. The school website and other online content published by the school

- The school website will not include the personal details, including individual e-mail addresses of staff or pupils.
- A generic contact e-mail address will be used for all enquiries received through the school website.
- All content included on the school website will be approved by the head teacher before publication.
- The content of the website will be composed in such a way that individual pupils cannot be clearly identified.
- Staff and pupils should not post school-related content on any external website.

21. Dealing with online safety incidents

- All online safety incidents are to be reported to the online lead using the purple Online Safety Incident forms (located in the staffroom), and will be recorded on the online safety log.
- Whenever possible evidence is to be saved in the online safety incident log.
- All allegations will be taken seriously and investigated.

Flowcharts for Managing an Online Safety Incident



Policy on the use of Social Networking Sites

https://www.suffolk.gov.uk/assets/community-and-safety/staying-safe-online/E-safety-incident-

1. Purpose

- This policy on social networking websites is in addition to the School's existing policy on email and internet use or Acceptable Use Policy. It takes account of the ACAS guidance on Social Networking.
- In this policy 'staff' means employees, volunteers (including governors), agency staff or anyone working within the school and using the school's IT equipment.
- In addition, the 'Nolan Principles' apply to all staff and will sit alongside this policy.
- The revised core standards for teachers (implemented September 2012), regarding expected behaviour in and outside of school, apply to this policy. The school expects all staff to abide by these standards.
- As staff are aware, the internet is provided (primarily) for school use. We recognise however, that many employees may rarely use the internet for personal purposes while in school. We also recognise that many employees participate in social networking on websites such as Facebook, Twitter, MySpace, Bebo and Friendster outside of work.
- The purpose of this policy is to outline the responsibilities of staff using the internet to access social networking websites.
- This policy applies to all staff using the school's IT equipment.

2. Personal use of the internet

- The school restricts and monitors access to social networking websites from its computers at all times. Access will only be allowed where use of such websites is for school purposes.

3. **Personal conduct**

- The school respects staff's right to a private life. However, the school must also ensure that confidentiality, its pupils, employees, volunteers, and its reputation are protected. It therefore requires staff using social networking websites to:
    - use caution when posting information on social networking sites and blogs
    - refrain from identifying themselves as working for the school
    - ensure that they do not conduct themselves in a way that is detrimental to the school; and
    - take care not to allow their interaction on these websites to damage working relationships between members of staff, pupils at the school and their families, and other stakeholders or working partners of the school
- If staff become aware of inappropriate material/comments they should notify the Headteacher as soon as possible, and if possible provide print outs of the comments made or of the pictures displayed.
- Staff must not be 'friends' or communicate with, students on any social network sites or similar websites, including, but not limited to, 'Facebook', 'Myspace', 'Twitter' etc. If any student makes

contact with any staff member, they must notify the Headteacher as soon as possible without making a response. Similarly, if any member of staff or individual associated with the school makes unintended contact with a pupil, it must be notified to the Head Teacher as soon as possible. In the absence of the Head Teacher a member of the SLT must be contacted. The Headteacher can then deal with the situation as appropriate.

- Staff are reminded that bullying and harassment against any other member of staff via social media sites is taken as seriously as workplace bullying and harassment. Any allegations will be dealt with under the schools' normal bullying and harassment or disciplinary policies, as appropriate and may also be treated as a criminal offence.

- Employees that post defamatory statements that are published on the internet may be legally liable for any damage to the reputation of the individual concerned. As a representative of the school, any statement made by employees could mean the school is vicariously liable for those statements if done in the course of employment, even if performed without the consent or approval of the school. The school takes these acts seriously and disciplinary procedures will be invoked if any such defamatory statements are made by its employees, which may lead to dismissal.

- In the case of Governors, whilst volunteers and not subject to disciplinary procedures, referral to Governor services in the Local Authority will be made and their advice and guidance will be taken.

4. Monitoring of internet access at work

- We reserve the right to monitor staffs' internet usage, but will endeavour to inform an affected individual when this is to happen and the reasons for it. We consider that valid reasons for checking a member of staff's internet usage include suspicions that they have:

    - been spending an excessive amount of time viewing websites that are not work-related; or
    - acted in a way that damages the reputation of the school and/or breaches confidentiality
    - contravened safeguarding policies or given cause for concern about their suitability to work with children

- The school reserves the right to request information regarding members of staff's use of the internet from our IT Support Technician or Internet Service Provider (ISP)

5. Disciplinary action

- If the school monitors staffs' internet use to ensure that it is in accordance with this policy, access to the web may be withdrawn in any case of misuse of this facility.

- If appropriate, disciplinary action will also be taken in line with the school's disciplinary policy.

6. Security and identity theft

- Staff should be aware that social networking websites are a public forum, particularly if the individual is part of a "network". Staff should not assume that their entries on any website will remain private. Staff should never send abusive or defamatory messages.

- Staff must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, staff must:

    - ensure that no information is made available that could provide a person with unauthorised access to the school and/or any confidential information; and
    - refrain from recording any confidential information regarding the school on any social networking website

- Publishing of information on social network sites should be assumed to be in the public domain as this will be assumed in all cases of breach of the policy.

- We ask all staff to consider the following before posting information or images on social networking sites:

    - Think carefully before posting information – would you want your employer or a potential employer to see it
    - Think carefully about who might see this, i.e. parents, pupils, the wider community, and what you do and don't want them to see
    - Review your information regularly – what may have seemed like a good idea at the time may not seem such a good idea some months or years later

Reception & Key Stage 1

Acceptable Use Agreement

Hopton Online Safety Rules

- I will only go on the internet when an adult has told me it is ok to do so.

- I will use the Internet to help me learn.
- I will learn how to use the Internet safely and responsibly.
- I will only send emails and messages that are polite and friendly.
- I will not talk or type messages to people I don't know on the internet.
- If I am sent a message from someone that I know that is unkind, nasty or hurtful I will tell a teacher or grown up I trust.
- If I receive a message sent by someone I don't know, I will tell a teacher or grown up I trust.
- I will never tell anyone on the internet anything about me, except my first name, unless my teacher says I can.
- I will not put photographs or video clips online unless my teacher has told me I can
- I will tell a teacher or grown up I trust if I see or hear something on the internet that I don't like or makes me feel upset or scared.
- I agree to look after myself and others by using my Internet in a safe and responsible way.
- I will use Google Classroom in a respectful way, remembering it is a platform for learning.
- My Google Classroom login is for me and not to be shared with others

Signed..... Date.....

Name..... (Printed)

Key Stage 2 Acceptable Use Agreement

Hopton Online Safety Rules

- I will only use ICT in school for school purposes and learn how to use the internet safely and responsibly.

- I will only send polite and friendly emails, using my class email address or my school email address when emailing.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will only email, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- I will only use online tools when asked to by a teacher or member of staff
- I will not give out my own details such as name, phone number or home address or the details of other I know
- I will not tell other people my ICT, including my Google Classroom, passwords.
- I will use Google Classroom in a respectful way, remembering it is a platform for learning.
- I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will only open and delete my own files.
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will tell a teacher or a grown up I trust if I am ever sent any unpleasant or nasty images or messages or if I receive any type of message from someone I don't know.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and my parent/ carer contacted if a member of school staff is concerned about my safety.
- I will not bring any mobile device into the classroom (mobile phone, iPad, tablet, smart watch) to school because I am not allowed to my use own devices in school. If I need a mobile phone for traveling reasons I will hand this into the office.
- I will not sign up to online services until I am old enough to do so. I understand I need parental permission to be on certain sites and that often social media sites have age restrictions to keep me safe.
- Whilst using ICT at home I will remember what I have been taught at school and be mindful of the content, contact and conduct of using the internet.
  ** **Content**: illegal, inappropriate or harmful content.
  ** **Contact:** harmful online interaction with other users.
  ** **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Signed..... Date.....

Name..... (Printed)

Acceptable Use Agreement - Staff, Governor and Visitors

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Online Safety Lead or Headteacher

- I will only use the school's email / Internet / Intranet / Learning Platform and related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of SLT or ICT manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer and member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I have read the Online Safety and Acceptable Usage Policy so that I can effectively deal with any problems that may arise through misuse by pupils, staff or myself.
- I will report accidental misuse.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I have read the Online Safety and Acceptable Use Policy so that I am aware of current Online Safety issue and can effectively follow procedures to deal with any incidents that may arise through misuse by pupils, staff or myself.
- I will report any incidents of concern for a child or young person's safety to the Senior Designated Person or Online Safety Lead in accordance with Online Safety Policy. If I have a concern about a member of staff I will report this to the Head teacher.
- I know who my Senior Designated Person and Online Safety lead is.
- I will not use personal electronic devices in public areas of the school between the hours of 8.30am and 3.00pm, except in the staff room or another room in the school where no children are present.

User Signature

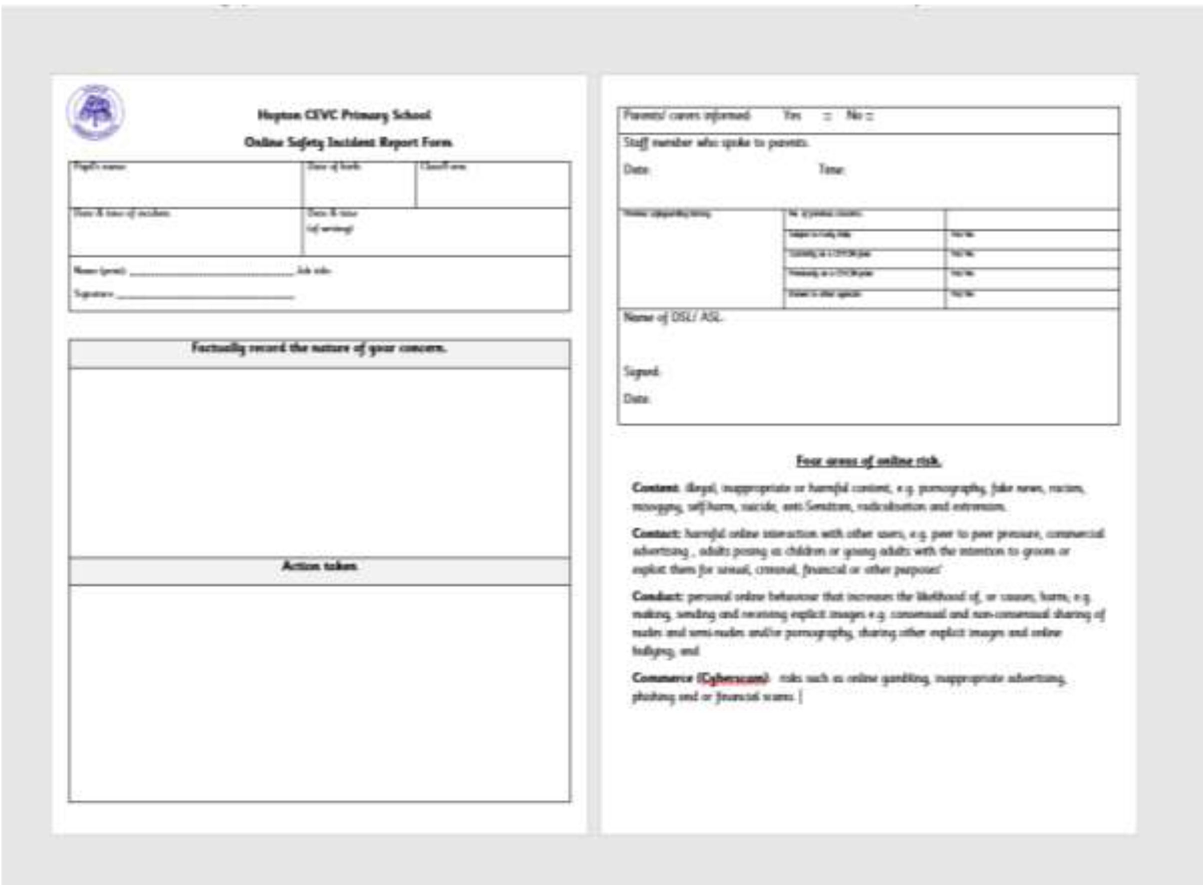
I agree to follow this Acceptable Use Agreement and to support the safe and secure use of ICT throughout the school in order to safeguard the pupils within our care.

Signature …… Date ……

Full Name …….... (printed)

Job title ……

Appendix 1: Online Safety Incident Report Form



Hopton CEVC Primary School

Online Safety Incident Report Form

Pupil's name	Date of birth	Class/Form
Date & time of incident	Date & time (of writing)	

Name (print): ______________________ Job title:

Signature: ______________________

Factually record the nature of your concern.

Action taken

Parents/ carers informed   Yes ☐ No ☐

Staff member who spoke to parents:

Date: Time:

Name of DSL/ ASL:

Signed:

Date:

Four areas of online risk.

Content: illegal, inappropriate or harmful content, e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: harmful online interaction with other users, e.g. peer to peer pressure, commercial advertising , adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'

Conduct: personal online behaviour that increases the likelihood of, or causes, harm, e.g. 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; and

Commerce (Cyberscams): risks such as online gambling, inappropriate advertising, phishing and or financial scams |