Upham CE (A) Primary School

Policy for E Safety

Approved by Governors – Curriculum Governors 19 May 2022

Review date – May 2025

1. Introduction to E-Safety

Digital technologies, including the internet, open up learning to children and their ability to explore and interact with the world. However, they can face many dangers using these technologies such as:

- Harmful, illegal or inappropriate content,
- Inappropriate communication with strangers or e-bullying,
- Risk of being targeted for grooming by those they make contact with,
- Loss of personal information,
- Inability to evaluate quality, relevance or bias,
- Excessive use affecting other development.

It is impossible to eliminate all risks completely so it is essential that we all teach children to understand the potential risks (in an age-appropriate manner that doesn't frighten them) and give them skills to manage the digital world with confidence. In addition children need to be aware of their digital footprint and the potential positive and negative impact of their digital actions on others.

In order to create a safe ICT learning environment, this policy details how the school has

- an infrastructure of whole-school awareness, designated responsibilities, policies and procedures
- an effective range of technological tools
- a comprehensive internet safety education programme for the whole school community.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour including Anti-Bullying, Safeguarding, Child Protection and GDPR

Our e-Safety Policy has been written by the school, building on County and Government guidance. It has been agreed by the staff and approved by governors.

The e-Safety Policy will be reviewed annually.

2. Context and Background

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- e-mail
- Instant messaging (often using simple web cams/ mobile cameras)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Video conferencing tools including virtual classroom platforms (Google Classroom)
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones/ tablets with camera and video functionality
- Smart phones with e-mail, messaging and internet access
- Online gaming; collaboration and in-game communication

Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools, including internet filtering;
- Policies and procedures, with clear roles and responsibilities;
- E-Safety teaching embedded into the school curriculum, schemes of work and wider activities.

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in Upham CE School and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school.

Leadership

The Headteacher ensures that the Policy is implemented across the school and takes ultimate responsibility for internet safety issues within school. He will also ensure an appropriate internet safety culture is created in school and that the governing body is informed of any issues.

E-Safety Co-ordinator

Our school E-Safety Co-ordinator is David Woolley (Headteacher).

He is responsible for keeping up to date on all e-Safety issues and ensuring that staff are updated and receive appropriate training as necessary. As DSL and behaviour-lead, he will also take the lead role in exploring suspected cyber-bullying as well as any safeguarding implications, building staff training into annual safeguarding training.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy. Governors will abide by the e-safety procedures set out in the governors code of conduct and will promote the highest levels of e-safety in their role, in their governance work and in all correspondence.

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Staff should ensure they are familiar with the school e-Safety policy, and ask for clarification where needed.

Staff are required to sign the Acceptable Internet Use agreement annually (See Appendix B).

Class teachers should ensure that pupils are aware of the e-Safety rules, introducing them at the beginning of each new school year and as points of teaching as they arise in both computer science learning and when ICT is used as a tool across the curriculum.

Teachers receive regular training, monitored by the Governing Body.

Children

Children are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school.

They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school. They also have a responsibility to report any incidents of misuse within school and to seek help from a trusted adult if they experience content or problems online which makes them feel uncomfortable.

Parents

Parents are given information about the school's e-safety policy and procedures via the school website where recommended self-help websites are listed and recommended. They are also given copies of the children's guidelines and asked to discuss, explore and support these rules with their children. As updates are received from other agencies in response to changing technologies/ reported misuse, relevant information will be passed onto parents via the weekly Newsletter to encourage communication, vigilance and awareness at home. Parents are also encouraged to share anything they are worried about, such as unsafe use of technology at home, with school staff so that school and parents can work together to support and protect children.

4. Technical and Hardware Guidance

Use of The Internet

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

The school uses HPSN2 – a flexible web filtering solution which enables schools to meet DfE requirements if used and managed at the school. Hampshire County Council provides a filtered internet feed that protects pupils from the viewing of inappropriate content. The service is provided via the Hampshire Public Services Network (HPSN). It uses a combination of methods to categorize sites, therefore providing a highly accurate system.

The filtering databases are updated every night, and in addition local blocking or unblocking of sites can be carried out by Hampshire IT in the event that an urgent change needs to be made. Updates are normally applied overnight but urgent changes can be made during the day after a request is processed through the IT Help Desk and then checked against the filtering policy. HPSN2 connectivity comes with managed firewalls and anti-virus software which protects schools from cyber threats and keeps children safe online.

However, no system is perfect and children would be encouraged to share any content which causes them concern (see Child responsibilities). Children are not permitted to use the internet without teacher's knowledge and permission.

An integral part of teaching children to become considered, reflective users of the internet is exploration and discussion around accuracy, validity and bias regarding information found.

Video Conferencing including Virtual Classroom Platforms

Video conferencing may be used by staff to enable assemblies or connect to visitors who cannot attend school. Staff will model safe use of this technology and reinforce important safety messages during use.

When used remotely by children, either independently or with an adult supervising (directly or from a distance), clear rules for use will be shared:

- You must make sure an adult knows you are joining a 'meeting',
- You must be in a shared space, such as a dining room, lounge, office or kitchen, not a bedroom.
- You must be dressed appropriately – not in pyjamas or bed wear.

These rules will be reinforced by staff during introductions, during live 'meetings' and through communication with parents. School Safeguarding procedures will continue to apply across video conferencing technologies.

Downloading files and applications

The Internet is a rich source of free files, applications, software, applications, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

Children are not allowed to download any material from the Internet and their individual login permissions are set up to not allow them to.

Portable Storage

Teaching staff, the headteacher and senior admin manager are able to access their desktops through encoded remote access. As a result, portable storage is not required and staff member must not use any device to save data which would be affected by General Data Protection Regulation (GDPR) (see staff acceptable use). If the use of storage device results in an anti-virus message, such as that used by a child to bring in homework, staff should remove the device and report this immediately to the headteacher. Before use, a virus scan should be completed for new temporary storage devices.

Technical ICT Support

The school uses Harrap Computer Systems Ltd to support the development and maintenance of our infrastructure. Staff will communicate with, liaise with and take advice from Harrap technicians regarding any concerns or issues.

Mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players. As part of E-Safety teaching within Computer Science, children will be taught the legal and moral implications of posting photos and personal information from mobile devices to public websites and how the data protection and privacy laws apply to their digital footprint. Children are not allowed to have personal mobile phones or similar devices in school or during school activities such as trips or residential visits.

5. Using ICT Safely

Contact details and privacy

Children's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian (see GDPR Policy for further details).

Pupils are taught that sharing this information with others can be dangerous.

As part of the ICT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based materials. Where pupil websites are published on the wider Internet, perhaps as part of a project, then identifying information will be removed, and images restricted.

Cyberbullying - Online bullying and harassment

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on children. Our school has a range of strategies and policies to prevent online bullying. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards in school.
- Pupils are taught how to use the Internet safely and responsibly (including awareness regarding age-restrictions), and are given access to guidance and support resources from a variety of sources.

- We encourage children to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.
- Complaints of cyber-bullying are dealt with in accordance with our Behaviour including Anti-Bullying Policy, with the headteacher taking the lead role.
- Complaints related to child protection are dealt with in accordance with school child protection policy and procedures.

Acceptable ICT use

Authorised Access

- All staff, governors and pupils must follow the 'Acceptable ICT Use' sections of this policy.

World Wide Web

- If staff, governors or pupils discover unsuitable sites, the URL (address), time, content must be reported to the ICT subject leader or network manager who will contact the Local Authority helpdesk to block said site.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Social Media

As a school we recognise that social media and networking are playing an increasing role within everyday life and that many staff and governors are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff, governors and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

As a school we block access to social networking sites on all school computers.

Staff and governors should:

- ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- not accept current or ex-pupils as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members are themselves parents of children at the school and as such have friends within the local community and ask that these members of staff take extra care when posting online and maintain professional conduct.
- ensure that their communication maintains their professionalism at all times.
- be aware that electronic texts can be misconstrued so should endeavour to minimise the possibility of this happening.
- not use these media to discuss confidential information or to discuss specific children.

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, individuals may be signed up with, or without, parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will ensure that parents are aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove such accounts or if any issues, such as cyber-bullying occur.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number.
- Staff, governors or pupils personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Digital and Video Images

We follow these rules to maintain safety on our school website:

- For a photograph of a child to appear on the site, consent must have been gained from the parent or guardian of the child. This consent is sought on admission and reviewed annually in September. A parent or guardian may choose to withdraw permission at any time.
- If we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure they are not left out of situations unnecessarily.
- We will not use the personal details or full names (which means first name **and** surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications.
- We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.
- Personal information about children or staff is not shared on our website. Contact e-mails are provided only for School office, Headteacher, and Website Administrator.
- All information on the school website is published by the headteacher or admin team. This avoids content on the website inadvertently contravening these rules.
- Photographs of swimming, changing for PE and other instances deemed inappropriate by class teacher will not be taken.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher. The school complaints procedure (published on website) will be used.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

6. What Parents Should Do If They Are Concerned About Their Child's Safety

Parents are encouraged to share any concerns with school staff. If parents require advice on how best to support their child develop more healthy or safer patterns of using ICT, they should share their concerns with the school DSL (David Woolley) who can offer advice and support and help to address the concern. Support materials, including organisations which could offer advice, are also detailed on the school website under the 'Our Curriculum' Tab then 'E-Safety'. During school holidays, the school email address adminoffice@upham.hants.sch.uk is regularly monitored so parents can raise concerns. Parents are also able to directly refer into children's services if they had concerns regarding another child or family.

If a child's safety is of concern, for example if a parent suspects potential grooming, radicalisation or inappropriate sharing of materials (such as sexting), then parents should contact the police directly in the first instance. It is important that electronic materials (such as phone texts or webchats) are not deleted as this valuable evidence trail could prove to be essential during an investigation and for tracing. It is also useful to take screen shots to preserve evidence.

7. Parents Protecting The Safety Of Others

Where parents (and other family memebers) are invited in for school events, they will be given advice and instructions regarding taking photographs or film on any device. It is reasonable to want to take photographs of your own children for private use but due consideration must be made for the identities and images of other children who may be captured or in the background. For some school events, specific instructions may be sought in writing. For other events where photography is likely to be wanted by parents, such as Christmas productions or Sports days, parents can expect clear communication around what is expected.

In general, the following rules must be followed by a parent for any event or visit:

> *In order for us as a school to allow such photographs to be taken we need to ensure due care and consideration is made to protecting the images of children other than your own that may be in an image. This involves that you ensure that:*
>
> - *Images containing children other than my own are not shared with any third party.*
> - *Images containing children other than my own are not sent electronically (which carries the risk of interception by a third party).*
> - *Images containing children other than my own are not put in a public space or electronic domain (such as Facebook).*

It would always be inappropriate for parents (or family members) to take photographs of your or any other children from outside of the school, such as whilst they are at playtime.

A helpful rule of thumb for any parent would be to make sure you 'know the rules before you start to take a photograph'.

If parents are observed to not comply with the communicated parameters, further actions would need to be required to protect the images of children, such as preventing parents taking photographs or direct communication with a parent to remove content from a social media post. In extreme case, advice may be taken from Hampshire County Legal Support Team.

Appendix A – E-Safety Rules for Children

EYFS & Key Stage 1

Think then Click

These rules help us to stay safe when I go online:

- **I only go online with a grown up.**

- **I am kind online.**

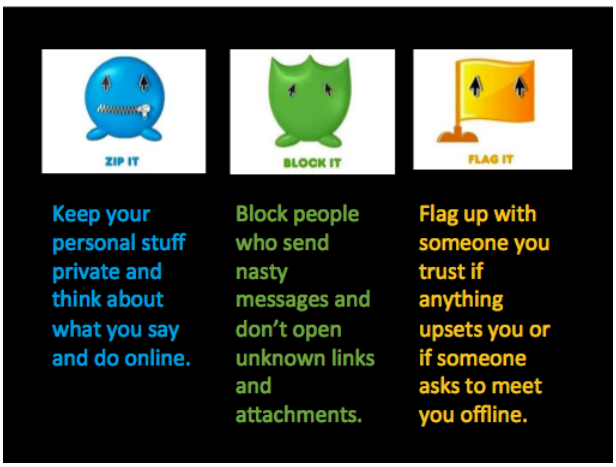
- **I keep information about me safe.**

- **I only talk to people online who I know in real life.**

- **I tell a grown up if something online makes me unhappy.**

Key Stage 2

- I will only use ICT in school for school purposes.
- I will not use a personal email address in scool.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my password.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not deliberately 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.



Appendix B – ICT Acceptable Use Agreement for Staff

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's E-Safety policy for Internet access for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I understand that I must not use the school ICT system to access inappropriate content
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems and hardware may not be used for private purposes without specific permission from the head teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. It must NOT be kept on removable storage devices.
- I will respect copyright and intellectual property rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead.
- I will ensure that electronic communications with pupils including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: …… Name: …… Date: ……

Accepted …… Name: ……
for school: