Wrenbury
PRIMARY SCHOOL

E-SAFETY POLICY

(This policy links to the Child Protection / Safeguarding policy and KCSiE 2023)

'We all matter'

Effective: Autumn 2023 **Review: Autumn 2024**

keep under review if changes needed

Person responsible for policy	FGB
Approval Date	September 2023
Chair of Governors	Terry Whalley

Introduction

Our e-Safety Policy has been written by the school. It has been discussed with staff, agreed by the senior management, and approved by Governors. It has considered the updated online safety aspects of KCSiE 2023 and links to the school's child Protection / Safeguarding policy. It will be reviewed every year or when guidance/legislation changes, whichever is sooner.

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 and school site.

This Policy document is drawn up to protect all parties: the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

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 (e.g. Rocket.chat; Instagram, MS Teams; Facebook Messenger; WeChat; Whtasapp)
- Web based voice and video calling (e.g.Facetime; Zoom)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. X and META)
- Podcasting (radio/audio broadcasts downloaded to computer, tablet, or phone)
- Video broadcasting sites (e.g. YouTube; Vimeo)
- Music and video downloading (e.g., iTunes; spotify)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging, and internet access

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
- Policies and procedures, with clear roles and responsibilities
- E-Safety teaching embedded into the school curriculum and schemes of work

Roles and Responsibilities

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

Leadership team

The SLT ensures that the Policy is implemented across the school via the usual school monitoring procedures.

e-Safety coordinator

Our school e-Safety coordinator is Bessa Cador, the Headteacher and Designated Safeguarding Lead, supported by the Computing Subject Lead, James Thorburn. They are responsible for keeping up to date on all e-Safety issues and ensuring that staff are updated as necessary.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy. The school's link governor for Safeguarding (including e-safety and Computing) is Andrea Sanders.

School Staff

Pupils

Pupils 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

Technical and Hardware Guidance

School Internet Provision

The school uses 'Computeam' to oversee its internet provision.

Content Filter

'Computeam' use a sophisticated content filter to ensure that as far as possible, only appropriate content from the internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- All pupils and staff have been issued with clear guidelines on what to do if this happens and parents will be informed as necessary.
- If staff or pupils discover unsuitable sites, the URL and content must be reported to the e-safety coordinator.
- Any material which the school deems unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk)
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

Downloading Files and Applications

The Internet is a rich source of free files, applications, software, 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.

- Pupils are not allowed to download any material form the Internet unless directed to do so by an appropriate staff member.

Portable storage media

Staff should use the USB storage as provided by school, wherever possible. If a teacher's own device is used, this should be checked regularly for any viruses. If any item is suspected of containing a virus, it should not be used, and the concern immediately reported to the technician.

Security and Virus Protection

The school subscribes to Panda Endpoint anti-virus software.
The software is monitored and updated regularly by the school's technical support through Apex Computing.

- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the office to log a 'ticket' with Apex support or conversely staff can do this themselves.

E-Safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At Wrenbury, we are committed to teaching pupils to use ICT effectively and appropriately in all aspects of the education; Awareness Days (eg annual Internet Safety Day in February and anti-bullying week including cyber-bullying in November) raise the profile of e-safety alongside lessons planned into the curriculum map for computing and RSE.

Internet Access at School

Use of the Internet by Pupils

Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the internet, and computers with Internet access are carefully located so that screens can be always seen by all who pass by.

Access for all Pupils

We want to ensure that all our pupils have access to the Internet, particularly where this will directly support a child's learning.

Out of hours Provision

The school's after school club, The Nest, runs from 3:30 - 6:00pm on Mondays and Tuesdays and from 3:30-4:30pm on Wednesdays to Fridays. Only supervised access to the internet is permitted during these times.

Using the Internet for Learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and as a source of digital learning materials.
We teach our children how to find appropriate information on the Internet, and how to ensure they understand who has made this information and how likely it is to be accurate and truthful.
Teachers carefully plan and check all internet-based teaching to ensure that all pupils are focused and using appropriate and relevant materials.
Children are taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary.
They are taught how to recognize the difference between commercial and non-commercial websites, and how to investigate the possible authors of web-based materials.

Teaching Safe Use of the Internet and ICT

At Wrenbury, we are aware of both the risks and benefits of technology and the increasing issues relating to its use, safety, safeguarding, and welfare including online and digital safety as referenced in KCSiE 2023. We plan and deliver online safety lessons using the CEOP 'uthinkuknow' resources to promote e-safety and educate the children in keeping safe online. When concerns are raised about a child's online safety as a perpetrator or as a victim, these should always be referred to the school's Designated Safeguarding Lead.

Suitable Materials

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognize that it can be difficult to navigate and find useful and appropriate materials. Where possible, and particularly with our younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children or using them in their teaching.

Non-Education Materials

We believe it is better to support children in finding their way around the internet with guidance and positive role-modelling rather than restrict Internet use to strict curriculum-based research. As well as internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-orientated activity sites that have interesting and relevant activities, games, and information, in free time, out-of-school provision and at home. Where external concerns are raised about a site, these are shared with parents via email or text.

Unsuitable Materials

Despite the best efforts of school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant, or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.
This action may include:

1. Making a note of the website and any other websites linked to it.
2. Informing the e-safety coordinator
3. Logging the incident (CPOMS)
4. Discussion with the pupil about the incident and how to avoid similar experiences in future.

Using E-mail at School

E-mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail and how to use it appropriately and effectively.

- We teach the use of e-mail as part of the Computing curriculum
- Pupils are ***not allowed*** to access personal e-mail accounts on school Internet facilities.
- Personal e-mail or messaging between staff and pupils should not take place
- Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.
- Incoming e-mail should be monitored, and attachments should not be opened unless the author is known.

Chat, Discussion and Social Networking Sites

These forms of electronic communication are used more and more by pupils out of school and can also contribute to learning across a range of curriculum areas.

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

We use the resources, guidelines and materials offered by CEOP 'uthinkuknow' to teach our children how to use chat rooms safely.

Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.
Pupils will be advised to use nick names and avatars when using social networking sites.
Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.
All commercial Instant Messaging and Social Networking sites are filtered as part of the LA Internet Policy.
Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

Internet-enable 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.

It is important that whist school recognizes the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog. Pupils do not use mobile phones or devices in school. Where a mobile phone is brought into school for travelling and safety reasons, this is always agreed with school and parents and the device, while the pupil is in school, is kept securely in the school office.

Cyberbullying – Online Bullying and Harassment

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chatrooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying (cyber-bullying), outlined in various sections of this policy.
Pupils will be taught the legal and moral implications of posting photos, semi-nudes, and personal information

from mobile phones to public websites etc. and how the data protection and privacy laws apply.
These include:

- No access to chatrooms, Instant messaging services and bulletin boards.
- Pupils are taught to use the Internet safely and responsibly and are given access to guidance and support from a variety of sources.
- Pupils are not allowed to have personal mobile phones or similar devices in school. Parents may request such devices are kept in the school Office for pupils who may need then on their journey to or from school.
- The sending of abusive or inappropriate text messages or files or nudes/semi-nudes by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's Anti-Bullying and Behaviour Policies.
- We encourage pupils 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 Anti-Bullying Policy.
- Complaints related to safeguarding / child protection are dealt with in accordance with school child protection policies.

Contact Details and Privacy

As specified elsewhere in this policy, a pupil's personal details, identifying informations, 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.
Pupils are taught that sharing information with others can be dangerous.

School and Pupil Websites – Pictures and Pupil Input

As part of the ICT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.
Any work that is published on a public website and attributed to members of our school community will reflect the school, and will therefore be carefully checked for mistakes, inaccuracies, and inappropriate content.
Pupils may design and create personal web pages. These pages will generally only be available to other school users or as part of a password protected network or learning platform.
Where pupil websites are published on the wider Internet, perhaps as a project with another school, organization etc., then identifying information will be removed, and images restricted.

Deliberate Misuse of the Internet Facilities

All pupils have discussed the rules for using the Internet safely and appropriately. Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous mistake.
Sanctions will include for:
-Unsuitable materials (e.g., online games, celebrity pictures, music downloads, sport websites etc.)

- Initial warning from the class teacher
- Banning from out-of-school-club internet use facilities
- Report to Headteacher
- Letter / phone call to parent – recorded on Pupil Concern sheet (uploaded to CPOMS)

-Offensive material (e.g., sharing or downloading pornographic images, racist and/or sexist comments or viewing hate website or images etc.)

- Incident logged (CPOMS) and reported to Headteacher
- Removal of Internet privileges/username etc.
- Meet with parent/carer
- Removal of Out of school hours access to Internet
- Subsequent incidents may be treated very seriously by the Headteacher and may result in police involvement and suspension or exclusion.

How will Complaints regarding E-Safety be handled?

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 apply to the school's physical building.

Due to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school or Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.
Sanctions available include:

- All incidents recorded (CPOMS)
- Discussion with class teacher, deputy headteacher and headteacher/e-safety coordinator
- Informing parent/carer
- Removal of Internet or computer access for a stated period
- Referral to LA / police

Our e-safety coordinator acts as a first point of contact for any complaint. Where a complaint is related to safeguarding, the complaint will be directed to the DSL.
Any complaint about staff misuse is referred to the headteacher.

Wrenbury Primary School

Pupil’s Acceptable Use of ICT:

- I will ask permission from an adult in school before using any ICT equipment (e.g., laptops, tablets, etc.), and only use it when a teacher or another adult is with me.
- I will only use the school’s IT for schoolwork, homework, and sites that a teacher/teaching assistant permits me to.
- I will not look at other people's files without their permission.
- I will use the usernames and passwords provided by the school to access platforms like J2E.
- I will not bring software or USB memory sticks into school without permission.
- I will ask permission before using the Internet, and only use it when a staff member is present
- I will only visit web sites that I am asked to by school staff, or that have been saved in a shared internet link folder for pupils to use.
- I will not use Google image search without being asked to do so by a school staff member.
- I will not download anything (files, images etc.) from the Internet unless given permission.
- I will only use an approved e-mail account provided for me by the school to send e-mail as part of my learning. I will not use personal e-mail accounts at school.
- The messages I send or information I upload as part of my schoolwork will always be polite.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information online that could be used to identify me, my family, or my friends, unless my teacher has given permission.
- If I see anything that makes me uncomfortable, or I receive a message I do not like, I will not respond to it, but I will immediately tell a school staff member.
- I understand that the school may check my computer files, e-mail, and the Internet sites I visit, to help keep me safe.
- I understand that if I deliberately break these rules my parents and the Headteacher will be informed.

Remote Learning

All schools are required to have a Remote Learning Plan and protocols for the staff, parents, and pupils to be aware of. The Remote Learning Plan has been shared with staff and the plan is published on the school website and can be found in the appendices.

Safeguarding:

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk.

Any such concerns should be dealt with as per the Child Protection Policy and where appropriate, referrals should still be made to the school's Designated Safeguarding Lead (DSL), who is the Headteacher or the Deputy DSLs or children's social care and if required, the police.

Schools will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

In the provision of online learning, the school has chosen to use Seesaw as its virtual learning platform (VLP)

Where video support is used, at Wrenbury it is **not live** videoing but is recorded and uploaded on to Seesaw. This is to protect both staff and pupils.

- Suitable/professional clothing should be worn by the teacher.
- The video should be recorded in an appropriate space.
- Language and behaviour must be professional and appropriate.
- Recorded videos will be for the sole purpose of supporting children's learning

Use of the Internet and ICT resources by school staff

The Internet

Our school understands that the internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

Internet Availability

To enable staff to make full use of these important resources, the internet is available in school to all staff for professional use.

ICT Equipment and Resources

The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, and a range of professional and curriculum software.

Professional use

Staff are expected to always model appropriate ICT and Internet use. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the internet, and to provide pupils with appropriate models to support the school's Diversity and Equal Opportunities policies as well as our Equality Objectives.

Staff who need support or CPD in using ICT as part of their professional practice can ask for support from the Computing Subject Lead.

Personal use of the Internet and ICT resources

Some equipment (including laptops) is available for loan to staff, with permission from the Headteacher. The appropriate forms and agreements must be signed. However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use. These are outlined in the staff agreement form below.

E-mail

We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies, and other groups.

Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

Online discussion groups, bulletin boards and forums, online chat, and messaging

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin boards to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and all communications must reflect this.

E-Safety Policy Staff Agreement Form

This document covers use of school digital technologies, networks etc. both in school and out of school.

Access

- I will obtain the appropriate log on details and passwords from the Computing coordinator.
- I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system.
- If my password is compromised, I will ensure I change it.
- I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access school ICT systems or resources.

Appropriate Use

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will never view, upload, download or send any material, which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous, or inappropriate sexual content.
- I will not download, use, or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-Safety coordinator.

Professional Conduct

- I will not engage in any online activity that may compromise my professional responsibilities
- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role
- I will never include pupils or former pupils as part of a non-professional social network or group
- I will ensure that I represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion, or posting to public websites using school facilities
- I will not browse, download, or send material that could be considered offensive to colleagues
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact

Personal Use

- I understand that I may use internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes.
- I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures, or other material onto school computers, or onto the school network area.
- I understand that the forwarding of e-mail chain letters, inappropriate 'jokes' and similar material is forbidden.
- I will not use the school Internet facilities for personal access to public discussion groups or social networking site

E-mail

- I will only use the approved, secure e-mail system for any school business
- I will only use the approved school e-mail, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

Use of School equipment out of school

- I agree and accept that any computer or laptop loaned to me by the school, is provided mainly to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
- I will return school equipment regularly (to be agreed with ICT Administrator) to be checked and updated

- I will not connect a computer, laptop, or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software

Teaching and Learning

- I will always actively supervise, or arrange for suitable supervision of pupils that I have directed or allowed to use the Internet
- I will embed the school's e-safety curriculum into my teaching, using agreed resources and materials
- I will ensure I am aware of digital safeguarding issues, so they are appropriately embedded in my classroom practice
- I will only use the internet for professional purposes when pupils are present in a classroom with Internet access

Photographs and Video

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission
- I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance)

Data protection

- I will not give out or share personal addresses (including e-mail), telephone/mobile phone numbers of any adult or students working at the school.
- I will not take pupil data, photographs, or video from the school premises without the full permission of the head teacher e.g., on a laptop, memory stick or any other removable media
- I will ensure that I follow school data security protocols when using any confidential data at any location other than school premises
- I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission
- I understand that GDPR data protection policy requires that any information seen by me regarding staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

Copyright

- I will not publish or distribute work that is protected by copyright
- I will encourage pupils to reference online resources and websites when they use them in a report or publication

User Signature

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I agree to have a school user account, be connected to the internet via the school network and be able to use the school's ICT resources and systems.

Signature .... Date...

Full Name .... (Printed)

Job title ....

Authorised Signature (Headteacher or Deputy Headteacher)

Signature.. Date...

Full Name.. (Printed)

GDPR Policy

Our school is aware of the data protection law as it affects our use of the Internet, both in administration and teaching and learning.

We adhere to the LA Guidelines on GDPR.

Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.

Staff Laptop and ICT Equipment loans

Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this e-Safety Policy.

This must be the case wherever the laptop, computer or other such device is being used as it always remains the property of Wrenbury Primary School.

Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy regarding protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense.

Staff must sign the 'Staff Laptop and Computer Loans Agreement' before taking the equipment away from the school premises.

Wrenbury
Primary School

Staff Laptop and ICT Equipment Loan Agreement

I have borrowed a school laptop to use out of school in agreement with both Head Teacher and the Computing coordinator.

Make:

Model:

Serial Number:

It is understood that I will return the equipment to school if requested to do so by either the Head Teacher or the Computing coordinator.

I undertake to take proper care of the equipment whilst in my possession and will abide by the requirements of the school's insurance policy regarding protecting the equipment from loss or damage.

I agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, I will replace (like for like) or arrange for the repair of the equipment at my own expense.

I will use the equipment in accordance with the schools e-Safety Policy and Staff Acceptable Use policy.

I agree to the above conditions.

Signature: **Print name:**

Date:

Headteacher's signature: **Print name:**

Date:

Date returned: **Signed back in by Headteacher:**