Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.
Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms (MLE) and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Varying mobile devices with web functionality.

At Colwall C of E Primary School we understand the responsibility to educate our pupils in E-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities

Promoting high standards of E-Safety is everybody's responsibility. As E-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.
The named E-Safety coordinator in our school is **Alex Paynter**.
All members of the school community have been made aware of who holds this post. It is the role of the E-Safety coordinator to keep abreast of current issues and guidance through organisations such as Common Sense Media, CEOP and 'Think U Know'.

The E-Safety coordinator updates the Senior Management Team and Governors. All Governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and reviewing the e-Safety Policy

This policy (for staff, governors, visitors and pupils), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies:

- Social Media
- Home-school Agreement
- Behaviour
- Health and Safety
- Child Protection and Safeguarding
- PSHE policies including Anti-Bullying.

Our E-Safety policy has been agreed by the Senior Management Team and Staff. The E-Safety policy and its implementation are reviewed annually.

E-Safety Skills and Development for Staff

- All members of staff receive regular information and training on E-Safety issues through the coordinator at staff meetings.
- All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All new members of staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All members of staff incorporate E-Safety activities and awareness at the start of every term as part of their computing teaching (see Knowsley Computing Scheme) and revisit E-Safety and Digital Literacy themes throughout the year.

Community use of the Internet

- External organisations using the school's ICT facilities and relevant internet connection must adhere to the e-Safety policy.
- Families are made aware that devices loaned out for use during COVID-19 lockdowns are explicitly for use for remote learning only.

Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach E-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access includes appropriate filtering to protect children in all year groups from potentially harmful content. In addition to this, teachers are advised to follow our computing scheme rigorously to avoid encountering potentially harmful content that has not previously been checked.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. All pupils and staff are regularly reminded of our approach to 'things we do not like': Zip It, Flag It, Block It.
- Research is a fundamentally difficult skill for a primary school child to master and where necessary approaches are taken to teach skills to locate, retrieve and utilise safe and appropriate content.

Managing Internet Access

- School ICT systems capacity and security will be reviewed regularly.
- Anti-Virus protection is updated regularly by EduTech.
- System security is overseen by our technicians (EduTech).
- All staff are aware of the need to contact EduTech to fix technical issues.

Zoom & Teams

- Pupils must use their own names as log-in credentials to help prove their identity to the teacher.
- Pupils and Parents must ensure that children are appropriately dressed and in a suitably safe environment for their respective Zoom/Teams call (silhouette mode is enacted in Teams).
- Teachers are directed to be diligent in accepting participants to calls and checking their identity immediately before controlling and directing 'muting' participants.

Published content and the school web site

- The contact details on the school website are the school address, e-mail and telephone number.
- Pupils' personal information is not published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Teaching staff must follow 'social media restriction lists' when uploading photographs and videos to class pages of learning activities.

Publishing Pupil's Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully in line with given permission by parents (collated by the office).
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Pupils' work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc.

Social networking and personal publishing

- The school blocks access for children to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate and or illegal (e.g. Facebook, WhatsApp) for primary aged pupils.
- Our pupils are asked to report any incidents of bullying to the school and are made aware of the appropriate steps in preventing and flagging such instances (Zip, Flag, Block).
- School staff are advised not to add children, or parents as 'friends' if they use these sites.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed access.
- Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school are sent to the school office and kept there until the end of the day.
- The sending of abusive or inappropriate text messages or emails outside school is forbidden.
- Staff will use a school phone where contact with pupils is required.

Protecting personal data

- The school will hold personal information on its systems for as long as individual members of staff remain at the school and remove it in the event of staff leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the Data Protection Act.
- Each teacher has the right to view personal information that the school holds and to have any inaccuracies corrected.

Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement (AUA) for pupils and abide by the school's e-Safety guidelines.
- Access to the Internet will be by directly supervised and to specific, approved on-line materials.
- All staff using a school laptop will be made aware of the schools Laptop Use Policy

Password Security

- Adult users are provided with an individual network username and password, email address and Seesaw (online learning) username and password, which they are encouraged to change periodically.
- All members of staff are aware of the dangers inherent in leaving the SIMS and FFT systems, for pupil-tracking and digital registers, open and of the importance of keeping passwords secret

- All members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the E-Safety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety coordinator
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints and concerns of a child protection nature must be dealt with in accordance with school child protection procedures. For example evidence of: inappropriate online relationships; a child watching pornography or any '18' films on a regular basis; online/digital bullying, harassment or inappropriate image sharing etc.
- Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the E-Safety policy to pupils

- E-Safety rules are integral to all computing and discussed with the pupils at the start of each term. All staff are aware that at least one dedicated e-safety lesson must be taught each term and at relevant points throughout e.g. during PSHE lessons/Anti-Bullying week/Safer Internet Day.
- Pupils will be informed that network and Internet use will be monitored**.**
- The school is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search
- Pupils are required to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme

Staff and the E-Safety policy

- All staff must sign the Staff AUP and a copy is kept on file.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- All members of staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school (see laptop use policy). Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Parents and the E-Safety Policy

- All parents, when their child joins the school, will be asked to sign the AUA for pupils giving consent for their child to use the Internet in school by following the school's e-Safety guidelines and within the constraints detailed in the school's e-Safety policy.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website or on the respective school Facebook and Twitter pages.
- Parents are encouraged to look at the school's E-Safety policy and any 'Acceptable User Agreements' (for KS1 & KS2)
- Parents are provided with any relevant published communications from CEOP or CommonSenseMedia – which are all circulated on social media platforms.

The Learning Platform and other home/school internet use

- All staff have been trained and given advice on how to safely and effectively use SIMS and FFT.
- Staff are given appropriate guidance and training in best using Zoom, Seesaw and Microsoft Teams safely during periods of COVID-19 related lockdown. Best practice is shared and modelled for teachers her aren't familiar on procedures.
- Parents will be informed about safe and appropriate Seesaw, Zoom and Teams use through appropriate policies, updates and newsletter communication.
- All children will be given a username and password to access secure resources and facilities on Seesaw – details can only be accessed again through dialogue with the school office or respective class teacher.
- School staff will monitor the use of Seesaw and school Facebook comments. Any misuse of the school social media comments will be reported to the Headteacher.

Monitoring and Review

This policy is implemented on a day-to-day basis by all school staff and is monitored on an annual basis by the E-Safety Coordinator (Alex Paynter).

This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the e-Safety Coordinator, Designated Safeguarding Lead (DSL). Ongoing incidents will be reported to the full governing body.

Reviewed : February 2022

Reviewed by the Health and Safety Committee.
Signed by:

Headteacher Date: _____

Chair of Health and Safety Date: _____