E-Safety Policy

Governors Meeting:	**26 June 2023**
Safeguarding Governor:	**Jane Owens**
Chair of Governors:	**Gail Webb**
Review:	**26 June 2024**

At Huxley C of E (Aided) Primary School we understand the importance that technology plays in the lives of our pupils. Whilst we teach and encourage our pupils to embrace new technology as it emerges, its use must be balanced by educating pupils to take a responsible approach.

The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The nominated e-safety officer in school is Rachel Gourley who is the first point of contact for any esafety related incidents. You can contact her via her email: head@huxleyprimary.cheshire.sch.uk

Teaching and learning

- Within the Computing Curriculum (National Curriculum 2014), are specific, statutory objectives for e-safety for both KS1 and KS2 which staff will plan, teach and assess.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what internet use is acceptable, what is not and given clear objectives for internet use. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate internet content. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

- School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be in accordance with BECTA (British Educational Communications and Technology Agency) and Cheshire West and Chester (CWAC) recommendations. All filtering is managed by CWAC using Smoothwall filtering

system. This blocks sites that fall into categories such as race hatred, gaming and sites of an illegal nature.

- The LA approved system for secured emails uses encrypted devices or secure remote access where staff need to access personal level data off-site.
- Pupils may only use approved email accounts on the school system. Pupils must immediately tell a teacher if they receive an offensive email. Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission. Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.
- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photo permissions are gathered for all eventualities including website, Facebook and media. These permissions sheets are updated half termly and also when any changed are made by parents/carers. These permissions are kept in each classroom in locked drawers.
- The school has filtered access to social networking sites via CWAC filter. Facebook has been unblocked to allow access for the school staff to add school content to those social network sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for pupils of primary age.
- The school will work with CWAC (Internet Service Provider) to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, and are kept in bags. Any staff needing to make any calls must do so in the designated space (staffroom)
- Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances. It is expected that phones remain with personal belongings and are kept safe. Should a member of staff realise that their phone may potentially have been lost or taken then they should immediately inform the office, who should record the exact time and date and notify the Headteacher.
- The sending of abusive or inappropriate text messages is forbidden, as is any other form of cyber bullying.

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. If needed, they must block their number or seek permissions from the Senior Leadership Team.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity, then it will only take place when approved by the Senior Leadership Team.
- If mobile phones are used for photographs, the photographs must be deleted the same day.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

- All staff must read the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All staff and pupils are granted Internet access.
- Access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials. Parents will be asked to sign and return a consent form agreeing to acceptable use policy guidelines on admission to school.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor CWAC can accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT provision, to raise awareness of any concerns related to inappropriate internet use and to establish if the e-safety policy is adequate and that its implementation is effective.
- 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. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaints procedure. Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- Should any issues regarding e-safety come to light, parents and pupils should email Mrs Rachel Gourley head@huxleyprimary.cheshire.sch.uk

- An incident record will be completed by a responsible adult at the earliest opportunity, on CPOMS. The e-safety nominated officer (Mrs Gourley) who will investigate, should be notified of this record/incident.
- The school will liaise with local organisations to establish a common approach to e-safety.
- An e-Safety team will be established, and they will hold a responsibility for enhancing e-safety throughout school and have pledged to raise awareness of safety issues with all school stakeholders.

Communications Policy

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and internet use will be monitored.
- All staff will be given the school e-safety Policy and its importance explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Parents' attention will be drawn to the School e-safety Policy and the school website e-safety page as well as pupil esafety pages, where further support materials can be found.

Review

- This policy reflects the consensus of opinion of the whole staff and governors/IEB and its implementation is the responsibility of all staff and governors. This policy should be considered alongside all other policies in school and will be evaluated in accordance with the policy review cycle

Responsibilities

School's Responsibility

- To teach about e-safety including safe use of electronic communication and social media
- To teach the productive, safe and positive use of digital technology through Computing lessons and across the curriculum
- To deal with bullying, including online bullying, in line with school policy
- To only use online content from sites and apps that is age appropriate
- To share only information and images, opinions and information that identify individuals in a respectful and positive manner and with permission in line with our data protection policy
- To keep children's phones in the office for those families who require exceptions to be made regarding school policy on mobile phones

Parents' Responsibility

- To consider the role model they are providing to their children

- To monitor their child's computer, phone and tablet use including messages sent and received
- To consider the advice for children and parents above
- To deal with inappropriate messaging between children outside of school (e.g. removing their child's access to phones or chat groups)
- To only allow children access to apps and websites that are age appropriate
- To not share images, information or opinions about children, parents or staff in school on social media without their consent
- To ensure phones are kept at home during the school day or make an appointment with the headteacher if they require an exception to be made for their child

Child's Responsibility

- To use electronic media in a safe, useful and kind way
- To follow the advice above and learning about e-safety from lessons in school
- To comply with our internet acceptable use policy when using school equipment during the day, and out of school hours if your activity could affect other children in school (messaging or sharing with them).
- To only access and use apps and sites that are recommended for children their age
- To not share any image, opinion or information about any other person without their consent
- Not to bring phones to school unless they have permission, in which case, they take the phone to the office in the morning and collect in the evening

Useful links, websites and articles

Further links and documents can also be on our website.

1. https://www.naht.org.uk/news-and-opinion/news/pupil-support-and-safeguarding-news/five-tipsfor-switched-on-conversations-about-technology/
2. https://www.bbc.com/ownit
3. https://www.childnet.com/resources/looking-for-kidsmart
4. https://www.net-aware.org.uk
5. https://parentzone.org.uk/article/5-things-parents-should-know-about-screentime?utm_source=Mailing%208%20Jan&utm_medium=email&utm_campaign=PZ%20screen%20time %20article
6. https://www.vodafone.co.uk/mobile/digital-parenting/?cid=vnty-vodauto/dvynfvtq(uv(bx)yjhjoneanzqtojth
7. https://www.nspcc.org.uk/keeping-children-safe/online-safety/
8. https://www.whoishostingthis.com/resources/e-safety/#page-1

9. https://www.ceop.police.uk/safety-centre/
10. https://www.thinkuknow.co.uk/4_7/
11. https://www.thinkuknow.co.uk/8_10/
12. https://nationalonlinesafety.com