



Policy approved by Head Teacher: Date:.....

Policy approved by Governing Body: (Chair) Date:

The date for the next policy review is



Acceptable Use and Online Safety Policy – March 2021

Introduction

Digital technology in the 21st Century is seen as an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Ewloe Green has identified the need to embrace the use of digital technology in order to equip our pupils with the digital competencies to access lifelong learning and enhance their employment opportunities in the future. At Ewloe Green learners will learn to be conscientious digital citizens who contribute positively to the digital world around them and who critically evaluates their place within this digital world. They will be prepared for and ready to encounter the positive and negative aspects of being a digital citizen and will develop strategies and tools to aid them as they become independent consumers and producers.

Roles and Responsibilities:

Online safety is an important aspect of strategic leadership within the school, the Digital Learning Manager, Headteacher and Senior Leadership Team have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Digital Learning Manager is responsible for coordinating online safety at Ewloe Green and keeping all staff updated. Governors have an understanding of the issues at our school in relation to local and national guidelines and advice. Ewloe Green has appointed a member of the Governing Body to take lead responsibility for online safety via the role of online safety Governor.

Online Safety and Staff

- All staff receive regular updated information and training on online safety issues when required from the Digital Learning Manager and/or outside agencies
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know the reporting procedure for any concerns
- All staff have agreed to and signed the school's Acceptable Use and Online Policy.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or school into disrepute, or if something is felt to have undermined confidence in their professional abilities.



Acceptable Use and Online Safety Policy – March 2021

Online Safety and Learners:

- All learners must agree to a pupil code of conduct, which will be displayed in all classrooms.
- Delivery of digital citizenship is a cross-curricular responsibility as part of the Digital Competence Framework. In addition, specific citizenship lessons (Digital Literacy resource from Hwb/Common Sense Media) will be taught by all staff each half term.
- Digital Leaders are established across the school to raise the awareness of digital citizenship via peer collaboration and pupil voice via enrichment assemblies, delivering lessons and drop in sessions.

Online Safety and Parents/Carers

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used online e.g. on the school website. Parents are to inform the Headteacher in writing if they do NOT give consent
- The school website contains useful information and links posted by the staff and to support online learning and online safety to inform and update parents

Community Use of the Internet

External organisations using the school's digital facilities must adhere to the online safety policy.

Cyberbullying Management

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details and procedures are set out in the school's anti- bullying and behaviour policy.

Managing Internet Access

Email

Email is an essential means of communication for both staff and pupils. Ewloe Green believe that pupils should be taught how to use email positively and responsibly.

- Pupils may only use the email account linked to their Hwb account which can be monitored by the Digital Learning Manager.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers.



Acceptable Use and Online Safety Policy – March 2021

Published Content and the School Website

The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information will not be published. The Headteacher and Digital Learning Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Learners' Images and Work

- On enrollment at school parents are asked to fill in a consent form so that images can appear on the school website or other publications.
- Images or videos that include pupils will be selected and used appropriately.
- Parents must write to the Headteacher if they do NOT give permission for their child's photograph or work to appear online. Otherwise it is considered that consent has been given. This consent is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where written consent will be required. Parents/carers may withdraw permission, in writing, at any time.
- Pupils' full names will not be used anywhere on the Ewloe Green website, or any other online accounts used by the school

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 insist that photographs/videos taken are of their own children only. Photos/videos that include images of other children must not be shared online unless permission has been granted from the parents of the other children.

Social Networking and Personal Publishing

- The school will block access to certain social networking sites to pupils
- Pupils and parents will be advised that the use of many social network sites outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them and we will advise them on how to keep safe whilst using these sites set passwords, deny access to unknown individuals and to block unwanted communications
- Staff wishing to use social media tools with students as part of the curriculum will risk assess the website/s before use e.g. YouTube
- Pupils are asked to report any incidents of cyberbullying to staff or a Digital Learning Manager (who will then report to staff). All incidents are logged electronically



Acceptable Use and Online Safety Policy – March 2021

- School staff are strongly advised NOT to add past or present pupils as 'friends' if they use these sites
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

Managing Video Calls e.g. Skype, Facetime, WhatsApp

- All video call equipment in the classroom must be switched off when not in use.
- Video calls will be always be supervised by a member of staff.
- Dialogue will be established with other participants before taking part in a video call. If it is a non school site it is important to check that they are delivering material that is appropriate for the class.

Managing Emerging Technologies:

- Emerging technologies will be examined for educational benefit and an informal risk assessment will be carried out before use in school is allowed
- Staff are expected to use cloud based storage rather than memory sticks to avoid loss of personal data related to staff or pupils.
- Pupils are strongly advised NOT to bring personal mobile devices/phones to school - unless there are exceptional circumstances. Any phones that are brought to school are handed in to the class teacher and kept until the end of the day

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be managed by Flintshire County Council.
- Security strategies will be discussed with FCC and MCC Digital.
- Personal data taken off site must be secure, saved in the cloud, devices must be password protected.
- Files held on the school's network are subject to checks by members of the SMT.

Managing Filtering

- Flintshire County Council provide a filtering service for all desktop computers laptops and iPads. Filtering follows Welsh Government guidelines. Lightspeed (via MCC) filter all iPads and MacBooks.
- Both filtering systems will block all sites considered inappropriate.



Acceptable Use and Online Safety Policy – March 2021

- Changes to the school filtering policy will be risk assessed by the Headteacher and the Digital Learning Manager.
- All breaches of filtering will be reported to the Digital Learning Manager and the Headteacher if necessary. Staff and pupils are aware of this procedure.
- The Digital Learning Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. We will work with the Flintshire County Council, Hawarden High School technicians, MCC Digital and the internet service providers to ensure systems are effective to protect pupils.

Protecting Personal Data

See Data Protection Policy

Password Security

Staff are provided with an individual network and Flintshire County Council login username and password which can be accessed from all desktop computers and iPads. Staff and pupils also have individual Google Drive and Hwb accounts. Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network by logging off or locking their computers when not in use. Administrator passwords are controlled by Flintshire County Council on networks accessed via desktops and MacBooks. For all other systems administrator passwords are controlled by the Digital Learning Manager.

Handling online safety complaints

Complaints of internet misuse will be reported to the Digital Learning Manager and/or Headteacher. All incidents will be logged and kept in the Safeguarding file, in the Headteacher's office. Complaints of safeguarding must be dealt with in accordance with school safeguarding procedures. Pupils and parents complaints procedure can be viewed on our school website www.ewloegreen.co.uk

Monitoring and Review

This policy, supported by the school's/Code of Conducts, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for Digital Learning, Home-school agreements, Behaviour, Safeguarding, and PSHE policies including Anti-bullying. The Acceptable



Acceptable Use and Online Safety Policy – March 2021

Use and Online Safety Policy has been written by the Digital Learning Manager, building on advice from professional outside agencies and Welsh Government guidance, and has been agreed by the Senior Leadership team, staff and approved by the Governing Body.

E Safety for any Adult Working with/for Young People

All staff, students and volunteers working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting. Information about any aspect of the pupil's education, care and family circumstances should only take part within clear and explicit professional boundaries.

All adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust. Teachers in particular should be aware of the Statement of Professional values and practice outlined by the GTCW.

Through the Internet and social networking sites in particular, information is shared with a very wide audience and quickly leaves the control of the person who first posted it. All adults working in an educational establishment should ensure that they do not share via the internet anything that may identify a pupil, the setting, their family or another member of staff or otherwise breach any data protection legislation.

All staff should also be careful not to share information or photographs on the internet which will cause themselves or colleague's embarrassment or which will bring the reputation of themselves or colleagues or the establishment into disrepute. Such inappropriate action will warrant consideration under the school's disciplinary procedure.

'Do not publish anything you would not want your mum, children or boss to see now or in ten years time!

Equality Diversity

We recognise diversity and the protected characteristics of our school community and adhere to the practices within the Strategic Equality Strategy Plan.

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Digital Learning Manager. The adherence of this policy is the collective responsibility of the staff.



Acceptable Use and Online Safety Policy – March 2021

Electronic Communication Rules for Responsible Use - Pupils

The school has installed computers with Internet access to help our learning.

These rules will keep you safe and help us be fair to others.

- + I will only access the system with the class identity and password, and only access Google Drive/Hwb with my own identity and password, which I will keep secret.*
- + I will not access other people's files.*
- + I will use the computers for school work and homework.*
- + I will not bring in external media devices (e.g. memory keys) from outside school unless I have been given permission.*
- + I will ask permission from a member of staff before using the Internet.*
- + I will only e-mail people I know or my teacher has approved. The messages I send will be polite and responsible.*
- + A file will only be sent with my e-mail message if it has been checked and is free from viruses and if my teacher has approved sending the file.*
- + I will not give my home address or telephone number or arrange to meet someone.*
- + I will not disclose any other person's name, address or any of their personal details.*
- + I will report any unpleasant material or messages sent to me.*
- + I understand that the school may check my computer files, including electronic mail messages, and may monitor the Internet sites I visit.*



Acceptable Use and Online Safety Policy – March 2021

Electronic Communication Rules for Responsible Use - Staff

The school has installed computers with Internet access to help our teaching and pupil learning. These rules will keep you and the pupils safe and help us be fair to others.

- ✚ I will only access the system with my own identity and password.
- ✚ I will only access Google/Hwb with the appropriate school/personal logons.
- ✚ I will not access other staff files without prior permission. This excludes shared documents such as policy documents etc.
- ✚ I will only use the computers for work related to school, i.e. lesson planning, creating resources etc.
- ✚ I will not bring in external media devices (e.g. memory keys) from outside school unless I have ensured they are virus free and backed up regularly.
- ✚ I will only use e-mail for school related business. The messages I send will be polite and responsible. A file will only be sent with my e-mail message if it has been checked and is free from viruses.
- ✚ I will not give my home address or telephone number or arrange to meet someone.
- ✚ I will not disclose any other person's name, address or any of their personal details.
- ✚ I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect myself and other staff and pupils.
- ✚ I understand that the school/LA may check my computer files, including electronic mail messages, and may monitor the Internet sites I visit.
- ✚ I will comply with the School's social networking policy and procedures at all times

A copy of this document will be kept by the person responsible for ICT, signed by all staff who have computer/internet access.

