Online Safety Policy 2021-22

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, Broughton Primary School has identified the need to embrace the use of digital technology in order to equip learners with the digital competencies to access lifelong learning and enhance their employment opportunities in the future. At Broughton Primary School learners will learn to be conscientious digital citizens who will be able to think critically and contribute positively in the online 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.

Please refer to the Blended and Remote Learning policy in the event of school or class closure due to Covid-19.

Roles and Responsibilities:

Online safety is an important aspect of strategic leadership within the school, all staff have responsibility to ensure that the policy and practices are embedded and monitored. The Digital Leader is responsible for coordinating online safety at Broughton Primary School and keeping all staff updated. All Governors have an understanding of the issues at the school in relation to local and national guidelines and advice.

Online Safety and staff

- All staff receive regular updated information and training on online safety issues
- 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 agreement. (See Staff Online Acceptable Use Agreement)
- All members of staff are 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

Online safety and learners:

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) will be taught each half term. The eCadet team are established and raise awareness of digital citizenship via peer collaboration and pupil voice via assemblies, delivering lessons and drop in sessions.

Under GDPR regulations, 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, YouTube, Seesaw, Twitter etc. The school regularly uses it's Twitter feed to share useful information and links to support online learning and online safety to inform and update parents.

Community use of the internet

External organisations and/or individuals 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 learners. Broughton Primary School believe that learners should be taught how to use email positively and responsibly.

- Learners will only use their Hwb email account
- Staff will only use their Hwb email accounts to communicate with learners and parents/carers

Published content and the school website

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

Publishing learner's images and work

- Images or videos that include learners will be selected and used appropriately
- Due to GDPR regulations, consent must be sought from parents/carers before learner's photographs can be published online. This consent is considered valid for the entire period that the learner attends this school. Parents/carers may withdraw permission, in writing to the Headteacher, at any time
- Learners' full names will not be used anywhere on the school 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 advise that photographs/videos should only feature their own child/children. 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 learners
- Learners and parents will be advised that the use of many social network sites outside school is inappropriate for primary aged children. However, we accept that many learners will still use them and we will teach them skills to keep safe whilst using these sites
- Staff wishing to use social media tools with learners as part of the curriculum will use their professional judgment and risk assess the app or website before use
- Learners are asked to report any incidents of cyberbullying to staff or an eCadet (who will then report to staff). Incidents are logged electronically via CPOMs
- School staff are strongly advised NOT to add past or present pupils as 'friends' on social media
- Concerns regarding learners' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers where appropriate

Managing video calls e.g. Teams and Google Meet

- Video calls will be through Teams or Google Meet as recommended by Welsh Government
- 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
- When connecting with externals organisations, dialogue will be established with other participants before taking part in a video call. If it is a non school site, staff will check that the material being delivered is appropriate for learners

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 permitted
- Staff are expected to use password protected cloud based storage to avoid loss of personal data related to staff or learners. (See data protection policy)
- Learners are strongly advised NOT to bring personal mobile devices/phones to school. Any phones that are brought to school must be switched off and handed in to the class teacher until the end of the day.

Information system security

- School digital systems capacity and security will be reviewed regularly
- Virus protection will be managed by Flintshire County County (FCC)
- Security strategies will be discussed with FCC
- Personal data taken off site must be secure, saved in the cloud and devices must be password protected
- Files held on the school's network, Google Drive and Teams are subject to checks by members of the Senior Leadership Team

Managing filtering

- Flintshire County Council provide a web filtering service via Smoothwall for all devices. Filtering follows Welsh Government guidelines.
- Changes to the school filtering policy will be risk assessed by the Senior Leadership Team
- All breaches of filtering will be reported to a member of the Senior Leadership Team
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. We will work with FCC to ensure systems are effective to protect learners

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. Staff and learners also have individual Hwb accounts. Learners 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. Administrator passwords are controlled by FCC or the Hwb team (Welsh Government).

Handling online safety complaints

Complaints of online misuse will be reported to a member of the Senior Leadership Team. All incidents will be logged electronically. Complaints of safeguarding must be dealt with in accordance with school safeguarding procedures. Learners and parents complaints procedure can be viewed on the school website.

Monitoring and review

This policy, supported by the school's Acceptable Use Agreements, 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. Our online safety policy has been written 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.

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

This policy was updated in September 2021 and shared with staff. The date for the next policy review is **September 2022** or sooner if required.

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

Policy approved by Governing Body: …….. (Chair of Governors) Date: ……..