

E Safety Policy

Bryn Primary School



Aspire. Believe. Challenge.
Anelu. Credo. Herio.

Policy history:	Date: September 2020
Written	Reviewed September 2021
Agreed by Governing Body	September 2021



Rationale

Great importance is placed on teaching the safe and appropriate use of ICT and this is embedded within the curriculum. New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside schools. The Internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils to learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. An E-Safety Policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside of school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or music files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person
- Many of these risks reflect situations in the offline world and it is essential that this E-Safety Policy is used in conjunction with other school policies (e.g. Behaviour, Anti-Bullying and Child Protection Policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which

they may be exposed, so that they have the confidence and skills to face and deal with these.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Coverage

Bryn Primary School provides internet access, desktop computers, mobile devices and online collaboration capacities. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed. 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 outside of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Governors

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy.

Headteacher

The Headteacher is responsible for ensuring the safety, including e-safety, of members of the school community. The Headteacher is the named Child Protection Officer, which includes a responsibility for e-safety.

The Headteacher and SMT are responsible for:

- Ensuring that staff receives suitable CPD to enable them to carry out their e-safety roles and to train other colleagues.

- Following correct procedure in the event of a serious e-safety allegation being made against a member of staff.

Local Authority

The school's ICT is managed through Caerphilly LA Team. They are responsible for:

- Ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Ensuring that the school meets the e-safety technical requirements outlined in the relevant Local Authority E-Safety Policy and guidance.
- Ensuring that users may only access the school's networks through a properly enforced password protection policy.
- Ensuring that the use of the network, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher.

Teaching and Support Staff

All staff are responsible for:

- Ensuring that they have an up to date awareness of e-safety matters.
- Reading and adhering to the school's e-safety policy and practices.
- Reporting any suspected misuse or problem to the Headteacher.
- Ensuring any digital communications with pupils are on a professional level and only carried out using official school systems.
- Ensuring that e-safety issues are embedded in all aspects of the curriculum and other school activities.
- Ensuring that pupils understand and follow the school e-safety and acceptable use policy.
- Monitoring of ICT activity in lessons and extended school activities.
- Teaching children so that they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Ensuring pupils are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and they monitor their use and implement current school policies with regard to these devices.
- Using suitable sites during planned lessons.

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy.
- Have a good understanding of research skills and the need to avoid plagiarism to uphold copyright regulations.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices.
- They should know and understand school policies on the taking/use of images and on cyber bullying.
- They should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the schools E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through meetings, letters, website and information about national and local e-safety campaigns.

Usage Policies

All ICT users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Mobile Devices

The school provides staff and pupils with mobile computers and devices. These devices are to promote learning both inside and outside of the classroom. Staff and pupils should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Staff and pupils are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage or malfunction to the ICT Coordinator immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices, including use of the school network, may be monitored. Personal mobile phones must not be used in the classrooms and public areas.

Downloads

For the security of our network, download files from reputable sites and only for educational purposes.

Use of Digital and Video Images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing and publication and distribution of images on the internet.

Staff are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. Care should be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website or else where that include pupils will be selected carefully. Pupils full names will not be used anywhere on the website or Twitter accounts. General photographic permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Etiquette

Users should always use the internet, network resource and online sites in a courteous and respectful manner. Users should recognise that among the valuable content online is unverified, incorrect or inappropriate content. Users should use trusted sources when conducting research via the internet. Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleagues or employers to see. Once something is online, it's out there and can sometimes be shared and spread in ways you never intended.

Access

Bryn Primary at the time of writing does not provide its pupils with access to Twitter. Twitter is to be accessed from school devices by Teachers at the school and staff should avoid using their own personal equipment.

What is Twitter?

Twitter is a service that delivers bite-size chunks of information in 140 characters or less and allows you to connect and engage and collaborate with others for a variety of reasons. Tweets tend to reference people, places, and/or activities.

The Purpose of Twitter

The main site is used to "broadcast" learning experiences and achievements to parents and the community. This is a one-way flow of communication to parents to broadcast news and events, important information, informing parents of homework set and deadlines. The aim

of this is to run alongside more traditional methods like sending updates via seesaw, and not to replace it.

Control of Content on Twitter

The school Twitter account will be ran from school devices by Teachers only. Senior Management Team will run the main Bryn Primary Twitter account.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998, which states that data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

The Use of Twitter

The school Twitter is set as private. Tweets will only be seen by those who follow us. People we do not follow cannot direct message us and our tweets cannot be retweeted.

- All activity over Twitter may be monitored and retained.
- The school Twitter account will only tweet between the hours of 8am and 6pm between Monday and Friday. The only tweets outside of this time are for school events (e.g. football matches, residential trips, performances), homework support or to share urgent school news (e.g. closures due to adverse weather),
- No personal staff accounts are to be associated with school accounts on Twitter.
- To school Twitter account will only follow educationally linked accounts. No personal accounts, unless they are educationally linked, will be followed. For example a children's author.

- The school Twitter accounts will not reply to any 'replies' on Twitter. This is not the platform to discuss or debate school related issues.
- The school Twitter account will only use children's first names when referencing children.
- The school Twitter account will use Twitter to share positive messages about the school.
- The school will change the Twitter account password on a yearly basis.
- Individually targeted content will not be posted e.g. "Well done Josh a better lesson today". Tweets referring to a class along the lines of "don't forget the..." are acceptable. Although always think about the most effective way to communicate important information.
- Use of @twittername of other is to be avoided.
- By endorsing Twitter to broadcast information, we do not encourage use of Twitter by pupils. We do however promote e-safety rules such as "never write anything online that would be potentially upsetting; make sure you know how to report to anything you find that disturbs you; be careful who you talk to they may not be all they appear; never meet anyone online without telling parents" etc.
- Users should not plagiarise content, including words or images, from a school Twitter account. Users should not take credit for things they didn't create themselves or misrepresent themselves as an author or creator of something found online.
- If a tweet has @brynprimarypont in it, the account holder will be notified when it is sent. The account holder can use this to engage directly with the person who has tweeted. At Bryn Primary School, our Twitter purpose is to broadcast and not to engage directly with individual parents/community members.
- Private messages between you and the person that you want to receive the tweet are known as Direct Messages. Other people that are following you cannot see these messages. In order to send a DM you have to be following that account and they have to be following you. At Bryn Primary School, our Twitter purpose is to broadcast and not to engage directly with individual parents/community members.
- When you press 'Retweet' their username is automatically added. At Bryn Primary School, we will only retweet tweets from other classes within our school and our main account. Education related retweets may be retweeted if appropriate for parents and the community from the main account only.
- Users of Twitter and followers of school Twitter accounts are expected to alert the Head Teacher/Deputy Head Teacher/ICT Coordinator immediately of any concerns for safety or security.

Twitter Accounts

If staff are provided with access to Twitter accounts, they should be used with due care. Staff should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by this policy. Staff will be expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Twitter posts may be monitored and archived indefinitely.

Followers of Twitter

Followers under the age of 18 will not be allowed to follow any accounts within the school. When follow requests come through, an informed decision will be made on a case by case basis as to accept or decline. These decisions will be based on a number of factors:

- The name of the individual as read on their Twitter account and whether this name correlates to that of a parent on the SIMS database; is a school governor is a known and proper person to the SLT and ICT Coordinator.
- The quality of the biography of each individual as read in the bio section of their Twitter account.
- The images on view in the potential followers Twitter account.

In most cases, on or more of the above will be enough to accept a follow request.

In the unlikely event that a parent or other suitable follower is inadvertently rejected, the SLT or ICT Coordinator will hear each individual on a case by case basis. These hearings will usually involve the prospective follower making themselves known in person to the above names persons with their Twitter details and should take no more than a few minutes.

In order to protect itself from inappropriate content being distributed into its news feed, the school will not actively seek to follow other users. However, exceptions may be made where following an @ handle has obvious benefits to the school. Once again, these will be decided on a case by case basis at the discretion of the SLT and ICT Coordinator.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, impersonating, excluding and stalking are all examples of cyberbullying. Engaging in these behaviour or any online activities intended to harm (physically or emotionally) another person will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that activities are monitored and retained.

Staff and pupils should refer to the Anti-Bullying Policy and relevant advice sheets for further clarification.

Inappropriate Content/Referencing

We welcome referencing, mentions or interactions that posit the school in a positive light only. Therefore, we deem any of the following as inappropriate:

- Offensive language or remarks aimed at the school, its staff, parents, governors or others affiliated with the school
- Unsuitable images or content posted online
- Images or text that infringe upon copyright
- Comments that aim to undermine the school, its staff, parents, governors or others affiliated with the school

Any inappropriate content will be deleted and its users will be removed, blocked and depending on the nature of the comment, reported to Twitter. Furthermore, incidents of a more serious nature may be reported to the appropriate authority.

Limitation of Liability

The school will not be responsible for damage or harm to persons, files, data or hardware. While the school employs strict filtering and other safety and security mechanisms, and attempts to ensure their proper functions, it makes no guarantees as to their effectiveness. The school will not be responsible, financially or otherwise, for unauthorised transaction conducted over the school network.

The policy will be reviewed annually or more regularly in the light of any significant new developments in the use of the technologies, new threat to e-safety or incidents that have taken place.

Headteacher:	Mrs J Khan	Date:	06.09.2020
Chair of Governing Body:	D.Gronow	Date:	06.09.2021