BERRIEW C. P. SCHOOL

E-safety Policy

Reviewed- Autumn 2024
Next review date- Autumn 2025

Introduction

At Berriew C.P. our e-Safety Policy relates to how we protect and teach children whilst using the internet.
The e-Safety Policy should be read in conjunction with the ICT Policy, Curriculum, Child Protection , Safeguarding, health and Safety, acceptable use Policy, the Positive Behaviour and the Anti- Bullying Policy.
The Head teacher and Governing body have a legal responsibility to safeguard children and staff and this includes online activity.

Aims
The aims of the Policy are:

- To promote safe use of the internet by pupils at our School ad at home.
- To enable the internet to be used safely and imaginatively at School to promote pupils achievement, to support the professional work of staff and to reinforce the School's Management Systems.
- To educate pupils about the risks of electronic social networking and on methods of safeguarding themselves and other from those risks.
- To support all members of the School community in complying with relevant legal requirements.

Teaching and learning

- The Internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide pupils 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.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

Internet use will enhance learning

- The school's Internet access is designed to enhance and extend education
- Pupils will be taught what Internet use is acceptable and 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 shown how to publish and present information to a wider audience.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be asked to sign the school's "Acceptable Use Policy" along with their parents or carer's.

Benefits of using the Internet in education include:

- access to worldwide educational resources;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data
- access to learning wherever and whenever convenient.

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 will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- Pupils will be taught how to report unpleasant Internet content.

Managing Information Systems

- The school will regularly review ICT (through the Self Evaluation Programme) and internet security via the LA. All stakeholders will consider the following when using the internet.
- School ICT systems security will be reviewed regularly and virus protection is updated regularly.
- Security strategies are discussed with the Local Authority and we are fully complaint with the latest technologies at all times.
- The server operating system must be secured and kept up to date.

The schools Broadband network is controlled by the LA.
The use of user logins and passwords to access the school network will be enforced.

How will email be managed?
Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools, for example.

- Messages sent using the schools email system should not be considered private and the school reserves the right to monitor all e-mail.
- Pupils are not allowed to use personal e-mail accounts to send messages out on the school system. Pupils may only use approved email accounts for school purposes.
- We actively encourage all pupils who use e-mails to inform a parent or teacher if they receive offensive or inappropriate e-mails.
- We teach children not reveal their personal details or those of others, or arrange to meet anyone without the specific permission of their parents.
- We also teach children that all incoming e-mail should be treated as suspicious and attachments should not opened unless the author is known to them.

- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Head teacher. Access in school to external personal email accounts may be blocked.

Excessive social email use can interfere with learning and will be restricted. Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be. The forwarding of chain messages is not permitted. Staff should not use personal email accounts during school hours or for professional purposes. Excessive social email use can interfere with learning and will be restricted. Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be. The forwarding of chain messages is not permitted. Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed?
Our school website (soon to be launched) is a good place to display work and activities and experiences and inspires children to engage in their learning. Publication of any information online should always be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher and members of the Senior Management Team will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- We encourage the children of Berriew C.P. to use the school website and to share this with members of the family
- Pupils' names will not be used anywhere on the website and particularly in association with photographs. Pupils need to be taught the reasons for caution in publishing personal information and images online.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.

How will social networking, social media and personal publishing be managed?
- We forbid the use of social networking sites in school.
- Members of staff should not engage in dialogue about the school with parents through the use of social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc. Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

How will filtering be managed?
- Berriew C.P. works in partnership with Powys County Council to ensure that our e-systems are up to date and set to the maximum level to protect children in school.
- If staff or pupils come across unsuitable on-line materials, the web site address, URL and a description of the inappropriateness of its content must be reported to the head teacher

who will report it to the appropriate agencies such as the Powys ICT desk (ictservicedesk@powys.gov.uk), Dyfed Powys Police or CEO P.

- Teachers should always evaluate any websites/search engines before using them with their pupils; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

How will risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school will not accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Dyfed Powys Police. Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

- Staff should are given the opportunity to develop a safe culture by discussing together any potential concerns in targeted staff meetings and INSET.
- Any illegal activity would need to be reported to the school Designated Child Protection Coordinator.

- The ICT Coordinator will record all reported incidents and actions taken in the School e- Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- 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 (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet

Parents' and carers' attention will be drawn to Berriew C.P. e-Safety Policy in the school prospectus.

How will e–Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school's behaviour and
  child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community?

- The school will be sensitive to Internet-related issues experienced by pupils out of school,
  e.g. social networking sites, and offer appropriate the internet and mobile phones is a positive and creative part of their everyday life advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will instruct any guest who needs to access the school computer system or internet on site.

How will Cyberbullying be managed?

Many young people and adults find that using Unfortunately; technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents

- gives head teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.
- Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on. Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- All incidents of cyberbullying reported to the school will be recorded. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- The Police will be contacted if a criminal offence is suspected.

How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by pupils is not permitted in school unless authorised by the school.
- Pupils are to hand in their mobile phones to their class teacher at the beginning of the school day safe keeping and it will be returned at the end of the school day.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour and anti-bullying policy. The phone or device might be searched by the Senior Management team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

Pupils Use of Personal Devices

- No devices are allowed in school unless consent has been granted by the Headteacher. Devices may be allowed in school from specialist services if they are to support the learning of pupils.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office.
- Mobile phones and devices will be released after discussing the issue with parents/carers. If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- 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.

- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, 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 Management Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work- provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

How will the policy be introduced to pupils?
The policy will be introduced in ICT lessons, regularly as reminders when using the internet and when relevant circumstances are encountered.

Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Orange Education: www.orange.co.uk/education
- Safe: www.safesocialnetworking.org

All users will be informed that network and Internet use will be monitored. Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

Staff and the e-Safety policy

- All staff will be given a copy of the School e-Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced
- Staff will always use a child friendly safe search engine when accessing the web with pupils
- 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 institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?
Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website. A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days. Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.

Safeguarding Designated Person
The Headteacher has had training in E-Safety issues and is aware of the potential for serious safeguarding issues to arise from:

- Sharing personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actualincidents of grooming
- Cyber-bullying

e-safety group
The e-safety group provides a consultative group that has wide representation in the school community, with responsibility for issues regarding e-safety and monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Management of the School website and Published Content including Pupil images:
The school maintains a website which celebrates pupils' work and provides a valuable and easily accessible source of information for parents and the community about the School, its policies and management. The IT coordinator and staff are responsible under the direction of the headteacher are responsible for the management and updating of the website and for ensuringthat the contenet is appropriate and in accordance with its policy. Personal information about staff or pupils will not be published on the website. Contact details will be limited to the School
CEOP (Child Exploitation and Online Protection Centre):
www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign:
http://clickcleverclicksafe.direct.gov.uk Kidsmart:
www.kidsmart.org.uk
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com