Carreghofa Primary School

E-Safety Policy

Carreghofa Primary School values the rapidly changing world of internet technology as an extremely useful source of information and communication. We believe that our whole school community will benefit from safe, guided internet usage. Recognising the potential dangers as well as the benefits of internet technology will ensure that our pupils, staff, parents, governors and the wider community have appropriate, effective and safe use of ICT at Carreghofa.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to world-wide education resources including museums and art galleries. Access to national learning platform.
- Inclusion in government initiatives such as the Virtual teacher Centre (VTC);
- Educational and cultural exchanges between pupils world-wide; access to experts in many fields for pupils and staff;
- Communication with support services, professional associations and colleagues;

How will Internet use enhance learning?

- Internet access will be planned to enrich and extend learning activities.
- Allow children and staff to access national learning platform and resources, in school and at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluating resources and retrieval.
- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.

How will pupils learn to evaluate Internet content?

- Training will be given to the children and parents each year using the CEOPS programme; Think you know.
- If pupils encounter material they feel is distasteful, uncomfortable or threatening, they should report the address of the site to a member of staff.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts on the school system. Pupils' email accounts are linked and limited to email addresses within the school's learning organisation (Hwb).
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone on e-mail communication.
- The forwarding of chain letters is banned.
- E-mail sent to an external organisation should be written, in collaboration with a teacher, carefully and authorised before sending. Children are not able to send emails directly from their email account an external organisation, only staff.

How should Web site content be managed?

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and, where possible, will not enable individual pupils to be identified.
- Written permission from parents will be sought before photographs of pupils are published on the school Web site and other school social media platforms.
- Only school staff will be authorised to add photographs to the website.

Are social networking, chat forums and newsrooms safe?

- Carreghofa has a Facebook Page, Instagram Page, Twitter Account which is used as an informal notice board and to celebrate success.
- Carreghofa's Social Media Platforms are monitored closely. Only those with admin responsibilities can add members.
- Pupils will not be allowed access to public or unregulated chat rooms.

How can emerging Internet uses be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

How will the risk be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 Powys County Council LA can accept liability for the material accessed, or any consequences of Internet access.

- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head Teacher will ensure that the internet policy is implemented and compliance with the policy monitored

How will filtering be managed?

- Powys County Council have a strong filter which prevents access to inappropriate material in school. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate and effective. Any inappropriate material discovered inadvertently will be reported to Powys County Council immediately.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation

Key area of Focus for Staff

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements,
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.
-

How will the policy be introduced to pupils?

- Instruction in responsible and safe use should precede Internet access.

How will staff be consulted?

- All staff must accept and sign an Acceptable Use Agreement
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- Staff development in the safe and responsible Internet use, and on school Internet policy will be provided as required.

How will ICT system security be maintained?

- The school ICT systems will be reviewed with regard to security.
- The school's ICT filtering system is filtered through Powys County Council
- Virus protection will be installed and updated regularly by Ceredigion ICT Support
- Personal data sent over the Internet will be encrypted or otherwise secured.

Password Security

- Staff and school files and systems are located securely in the Cloud, managed by Hwb.
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details.
- Password for staff and learner Hwb accounts comply with Hwb and Microsoft suggested password guidance.
- Should a password become compromised, staff and children must notify staff with admin rights in order to change.
- Parents are informed that children in lower school to have their school passwords available on a piece of card/ paper. The page of passwords will be left in their bag, available for use in school and home. The page will be monitored closely by staff, children and parents. Should the page become compromised, passwords will be reset immediately by staff with admin rights.

Reporting and Responding to an Incident

- All members of the school community will be made aware of the need to immediately report online safety issues/incidents
- Follow reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- If there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the normal school safeguarding procedures

- Data Protection Breaches will follow reporting routes, consistent with GDPR policy.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher. If it about the Headteacher, then the complaint is referred to the Chair of Governors and the local authority

Communication with Parents

- Internet issues will be handled sensitively to inform parents without undue alarm.
- Parents will be asked to sign an Acceptable Use Agreement form regarding their child's Internet access.

The school will take every opportunity to help parents and carers understand these issues through:

- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc

Digital and Video Images

- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published.
- Staff must not begin a video call with a learner(s) without another member of staff present.
- Should the need for live-streaming or video conferencing, staff, children and parents need to adhere to acceptable use agreement.

Parents and children need to agree:

- Any child participating with Live Video Calls will have to listen to instructions from their teacher, will mute their microphones and turn cameras off, when requested to.
- Not use language in written posts or display anything inappropriate.
- Be conscious of your surrounding and viewable environment and ensure nothing inappropriate is visible.
- Only use the feature when asked to and hosted by school staff.
- They will tell a teacher if something has upset you on screen.
- They understand if you break the rules, then you may not be allowed to use this feature again.

Guidance

This policy has been written and reviewed in line with the following guidance –

- The protection of children online (2011)
- 360 safe Cymru
- SWGFL
- CEOP's – Think You Know

Please view this policy in conjunction with the following policies;

Equal Opportunities

Child Protection

Teaching and Learning

ALN

Privacy Policy

GDPR Policy

This policy will be reviewed every three years. Date of next review: March 2024.

This policy has been agreed and ratified by:

The Governing Body

Signed _____ (Chair of Governors)

The Head Teacher

Signed _____(Head Teacher)

The School Council

Signed _____(Chairperson of the School Council)

Responsible Internet Use

Rules for Staff

The school computer system provides Internet access to students and staff. This Responsible Internet Use statement will help protect students, staff and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity only.
- Copyright and intellectual property rights must be respected.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner
- Legitimate private interests may be followed, providing school use is not compromised.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Individual user's Internet access may be monitored, including Web and e-mail use. Files on the school system may be examined or deleted.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the local authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Upper School Children's Acceptable Use Agreement

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that are suitable. If I find myself on an inappropriate website, I will leave it immediately.
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

- I will look after the devices I use and try not to alter the settings on any devices or try to install any software or programmes and tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.
- I will think about how my behaviour online might affect other people making sure I am polite and responsible when I communicate with others
- I will not take or share images of anyone without their permission.
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include being banned from using the internet and ICT equipment and conversations with your parents/ carers and, if behaviour is illegal, the police may be contacted.

Please complete the sections below to show that you have read, understood, and agree to the rules included in the acceptable use agreement.

I have read and understand the above and agree to follow these guidelines.

Name of Learner: Group/Class:

Signed: Date:

Lower School Children's Acceptable Use Agreement

This is how we stay safe when we use computers:

- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/tablet.

Signed (child):

Parent/Carer Acceptable Use Agreement

Parent/Carers Name:_____Name(s) of Learners_____

- As the parent/carer of the above learners, I give permission for my child to have access to the internet and to ICT systems at school.
- I know that my child has signed/ discussed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed:

Date:

Guided Educational Use

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the ability to communicate widely and to publish easily. Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Risk Assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they need to learn to recognise and avoid these risks – to become "Internet wise". Schools need to ensure they are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Pupils need to know how to cope if they come across inappropriate material.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and Associated communication technologies. The balance between education for responsible use, regulation and technical solutions must be judged carefully.

Appropriate Strategies

This document describes strategies to help ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

The Internet is becoming as commonplace as the telephone, TV or books and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. As a consequence a policy is required to help to ensure responsible use and the safety of pupils.