YSGOL CROSSGATES

CROSSGATES C.P. SCHOOL

E-Safety Policy

During this period of Home Learning due to Covid 19 the school continues to take its duty seriously around Internet safety. With this in mind staff will only post material from sites that are educationally sound. They will make use of such sites as HWB to deliver and assess work for pupils and Apps such as Schoop to inform parents or email.

Crossgates CP School

E-safety policy

E-Safety encompasses the use of new technologies, internet and electronic communications such as: mobile phones, collaboration tools and personal publishing.

The school's e-safety policy will operate in conjunction with other policies including:

- PCC Safeguarding Policy
- Positive Behaviour Policy
- Anti- Bullying Prevention
- Child Protection
- PSE Policy
- Curriculum
- Data Protection and Security

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies and clear guidance.

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

- To teach the children to use the internet safely under supervision, developing their skills and understanding in order for them to manage their own risk as they use the internet independently.

- Safe and secure broadband including the effective management of filtering.

- A member of staff being responsible for the implementation and monitoring of this e-safety policy.

- All staff to be involved in the implementation and management of e-safety, being vigilant to both their use of technology and the monitoring of pupils use in the context to their safeguarding responsibilities.

Introduction

Policy statement

This policy sets out this School's policy on social media and e-safety issues both inside and outside work and applies to school and its pre-school setting. The objectives of this policy are to:

• Set out the key principles and code of conduct expected of staff in this school in respect of use of social media and e-safety so that pupils and staff are safeguarded.

• Ensure that social media is used in a way that treats colleagues and members of this school community with professionalism and respect.

• Ensure that everyone at Crossgates School is protected from any malicious cyber bullying and misinterpretations which can arise from the unsafe use of social media.

• Ensure that that staff feel able to report any concerns about breaches of esafety to a nominated person for e-safety.

• Ensure that staff understand their responsibility to also protect themselves and the reputation of the school by using social networking sites responsibly outside work.

1.2 School staff have a responsibility to safeguard the welfare and best interests of pupils as well as to maintain public confidence in their integrity. It is therefore expected that they will adopt high standards of personal conduct both in and outside school to maintain the confidence and respect of their colleagues, pupils, and public in general and all those in the whole school community.

1.3 A guide to roles and responsibilities is contained at Appendix A 1.4 Safe practice also involves using judgement and integrity about behaviours in places other than the work setting. School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

1.7 In ratifying this policy the Governing Body is also approving the Code of Conduct for School's Staff in Relation To E-Safety contained at Appendix B.

The purpose of this policy is to:

- Through consultation with pupils establish the ground rules we have at Crossgates Primary School for using the Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of our discipline and PSE policies.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.
- Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be reported to staff immediately.

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 students 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.
- The school Internet access is designed expressly for teacher reference and pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- HWB is a learning platform for educators and learners to share resources, knowledge and experience across the whole of Wales.
- The children are taught the benefits of mobile technologies and how to use them safely.
- The school endeavours to create a consistent message with parents for all pupils and this in turn should aid the establishment and the future development of the school's e-Safety rules.
- However, staff are aware that some pupils may require additional support or teaching including the adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Managing Internet Access

- School ICT systems capacity and security is reviewed regularly.
- Virus protection is updated regularly.
- Pupils are not allowed to bring mobile phones to school.

- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

-

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive offensive e-mail.
- Pupils must not send offensive or inappropriate e-mails. This also applies when using Microsoft teams in HWB.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.
- The school reserves the right to access pupil e-mail accounts if a concern is raised regarding inappropriate content.

School web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- To ensure the safeguarding of all pupils, photographs or pupil names are never published together. It is encouraged not to publish individual photographs. Only first names or pupil's initials are used.
- Photographs that include pupils are selected carefully.
- Pupils' full names are not used anywhere on the Web site.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school Web site *(see Appendix for sample permission form)*.
- Pupil's work will only be published with the permission of the pupil and parents.

<u>Social networking and personal publishing</u>

Pupils-

- Children are discouraged from using social networking sites that are not age appropriate.
- Chat rooms are blocked.
- Pupils are told never to give out personal details of any kind which may identify them.
- Pupils must not attempt to gain access to another person/pupil account.
- Pupils are taught not to share passwords with other people.

Staff-

- Whilst the School respects the legal rights of all individuals, employees need to be aware that what they do and say outside of work can often compromise their position inside work. It is also important to note that other people's perceptions need to be considered when using social media.

Parents-

- Parent/carers use of social media- Parents/carers are expected to comment or post appropriately about the school and its staff at all times, whether using a school-based platform or their personal social networking sites. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. Persistent use of posts which are derogatory to staff and/or the school will be dealt with by the Legal Team of Powys County Council. Social networking activities refer to those activities conducted, such as blogging (writing personal journals to publicly accessible internet pages), involvement in social networking sites such as Facebook, and posting material, images or comments on sites such as You Tube, Snapchat, Twitter etc

Cyber Bullying (a form of bullying through the use of ICT)

An effective whole school approach to the prevention of cyber bullying should include:

- An agreed whole school understanding of cyber bullying
- Talking about cyber bullying
- Encouraging children to report any incidents of cyber bullying
- Promoting the positive use of technology
- Regularly monitoring the impact of this policy and the teaching and learning of ICT.

Responding to the incident of cyber bullying should be dealt with using the existing behaviour and bullying prevention policies and procedures. (*See appendix for further guidance*)

If cyber bullying takes place outside of school and has a negative impact on the orderly running of the school and/or might pose a threat to another pupil during school time or to a member of staff then the head teacher may take reasonable steps to mediate between the parties.

Managing filtering

- If staff or pupils discover an unsuitable site, it must be reported immediately to a member of staff or the e-Safety Coordinator.
- A member of the SLT ensures that regular checks are made to ensure that the filtering methods are appropriate and effective. .

Managing emerging technologies

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

Protecting personal data

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998. **Please see GDPR policy**

Acceptable Use

- All staff read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource. PLEASE ALSO READ STAFF CONDUCT AT END OF POLICY
- The school keeps an up to date record of all staff and pupils who have agreed to the Acceptable Use Policy.
- In Foundation Phase access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Pupils are asked to re-sign their agreement as they enter Key Stage 2.

Assessing risks

- The school takes all reasonable precautions to ensure that user’s access only appropriate material by using Powys’ filtering system.
- The school audits ICT provision on an annual basis to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Serious complaints of e-Safety misuse are recorded by the member of staff who receives the complaint and then reported to the head teacher.
- Any complaint about staff misuse is referred to the head teacher.
- Complaints of a child protection nature are dealt with in accordance with the school’s child protection procedures, PCC Safeguarding Policy and All Wales Child Protection Procedures.
- The school’s Complaints Policy is available to all parents.
- Pupils and parents will be informed of the complaints procedure

The Governing Body will ensure that:

• The school recognises its legal responsibility to protect staff from unlawful harassment as well as mental and physical injury at work.

• The school’s E- Safety and Social Networking Policy will be reviewed and monitored periodically so that staff, pupils and parents feel confident

• The school effectively supports e-safety.

The Head teacher will ensure that:

• The whole school community including staff, pupils and parents are signposted to information, policies and practice about e-safety.

• Staff are provided with information and professional development opportunities with regards to understanding, preventing and responding to cyber bullying.

• Where it is not the line manager or Head teacher, ensure that the school has a nominated person as an e-safety lead to oversee, manage the recording, investigation and resolution of cyber bullying incidents.

• Staff are clear about to whom who they report any breaches of e-safety. The nominated person as the E-safety lead will ensure that:

• Staff receive appropriate support to deal with and or respond to claims of cyber bullying or any other breaches of e-safety.

• Incidents are dealt with in a timely manner.

• Where appropriate and in agreement of the wishes of the person who has reported the incident, report the actions to the police.

• Powys County Council is contacted as appropriate.

Communications

Introducing the e-safety policy to pupils

- E-safety rules are posted in all classrooms and discussed with the pupils at the start of each year *(see appendix)*.
- As part of the school's e-Safety work all pupils and their parents are informed of the child exploitation and online protection centre: www.thinkuknow.co.uk

Staff and the e-Safety policy

- All staff have copies of the school's e-Safety Policy and know its importance.
- Staff are aware of their responsibility to safeguard all pupils in their use of technology in learning.
- The staff AUP is discussed and agreed at an annual staff meeting.

Enlisting parents' support

- Parents' attention is drawn to the school's e-Safety Policy in newsletters, and on the school Web site.
- The Pupil AUP is sent home during Reception and Year 3 for parents to discuss with their children, sign and return.
- Parents are requested to follow the school's complaints procedure and not use social media.
- Parents are made aware of any useful information regarding online safety.

Working with the Police

- The school works in partnership with the Schools Community Police Office as part of the schools e-Safety work.
- Some forms of cyber bullying behaviour may involve criminal offences and in these cases the school will contact the SCPO in line with the school's bullying prevention policy.

This policy will be review annually by the governors and staff or in light of new guidance.

- CODE OF CONDUCT FOR THE SCHOOL'S STAFF IN RELATION TO E-SAFETY The School's staff must:
- Communicate with pupils and staff in an open and transparent way using the school phone number and email address. (Personal e-mail addresses should never be given to pupils or parents.)
- • Keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents in a professional capacity. (There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle, or where staff are transport escorts or where for PTA purposes for example both staff and parents have exchanged personal numbers). Similarly, there are specific occasions where, as an exception, it is appropriate for staff to share details with parents, for example emergency contact details during school trips. These contacts/occasions however, will be easily recognised and openly acknowledged. In any other situation, or where a staff member is in doubt, such sharing must be sanctioned by the headteacher. Staff have a responsibility to make sure that any such contact is known to the senior leadership team.

  • Keep their mobile phone secure whilst on school premises. All mobile phones should be switched off or silent whilst staff are on duty unless there are good reasons that have been confirmed with a member of the senior leadership team.

  • Never 'friend' or otherwise connect with a pupil at the school where they are working onto their social networking site. There may be exceptions e.g. where a teacher's own children attend the school. All staff are expected to exercise professional caution and staff registered with the Education Workforce Council are required to comply with the Council's Code of Professional Conduct and Practice.

  • Never use or access social networking sites of pupils and should never accept an invitation to 'friend' or otherwise connect with a pupil other than where the exceptions above apply.

  • Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school's reputation is compromised by inappropriate postings (this should include past postings.)

• Be aware of the potential of on-line identity fraud and to be cautious when giving out personal information about them which may compromise their own personal safety and security.

• Never share their work logins or passwords with other people.

• Understand who can view the content on their pages of the sites they use and how to restrict access to certain groups of people. The following are not considered acceptable at this school: • Under no circumstances should staff make highly derogatory defamatory, rude, threatening or inappropriate reference to any staff member, governor, pupil, parent or school activity/event during their social use of the internet or other communication media. Positive or neutral references to individuals should only be made with that person's permission.

• The use of the school's name, logo, or any other published material without written prior permission from the Head teacher. This applies to any published material including the internet or written documentation.

• The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

• The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

• The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

E-safety policy –

Head–

Chair of Governors-

Date:

Reviewed: Staff 16.04.20 Govs: 20.04.20

Appendix

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.