Ysgol Harri Tudur

Henry Tudor School

E-Safety Policy

Policy Adopted by Governor Resources Committee: Autumn 2014
Review annually
Last reviewed: Autumn 2021
Next review: Autumn 2022

E-Safety Guidance - briefing note for Governors Resources Committee

Policy outline

1. Responsibility

The school has designated members of staff with e-safety roles who have operational responsibility for e-safety, this includes the Assistant Headteachers, Leader of Key Stage 5, Network Manager and Deputy Director of Maths, numeracy and ICT, and report to the Headteacher, who remains responsible for this strategy and its implementation.

The Headteacher's termly report to governors will contain details of any significant developments in e-safety and ICT systems, together with reports of any breaches of e-safety and actions taken as a result.

The governing body is responsible for setting and maintaining the overall policy. The e-safety policy and its implementation will be reviewed annually by the governing body. In so doing, governors should consider the views of staff and students.

2. Teaching and learning

2.1. Why is internet use important?

The purpose of internet use in school is to raise educational standards, to promote pupil/student achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning.

Internet access in school is an entitlement for all those students who show a responsible and mature approach to its use. Access may be withdrawn from students who misuse the internet.

Pupils/students use the internet widely outside school and the school will help them to learn how to evaluate internet information and to take care of their own safety and security.

2.2. Access and Filtering

The school seeks to provide students with quality internet access as part of their learning experience. Wireless Internet access will be widely developed and made available to students using school machines. There will be a gradual rollout of access through pupils/students' own devices, subject to acceptable and responsible use and the availability of bandwidth.

The school's internet access is designed expressly for educational use and has appropriate filtering. Sites with huge distraction potential and social media sites (e.g. Facebook, Twitter, gaming sites) will not be available to students. However, some of the sites – especially YouTube - contain valuable resources for teachers and pupils, so will be made available.

Staff should guide pupils/students in on-line activities that will support the learning outcomes planned for the pupils/students' age and maturity. Internet usage will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils/students.

2.3. Teaching pupils/students how to handle the Internet

Pupils/students will be given guidance on what internet use is acceptable and what is not and given clear objectives for internet use. Pupils/students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils/students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Pupils/students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils also receive e-safety awareness education within ICT and PSE lessons.

Pupils/students will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. E-Safety is an agenda item at School Council meetings for pupils to raise any new or emerging e-Safety issues they feel strongly about and any points raised are considered by the Deputy Director of Maths, numeracy and ICT.

3. Managing Information Systems

3.1. How will information systems security be maintained?

The security of the school information systems will be reviewed regularly. Virus protection will be updated regularly. Backup strategies (including off-line and off-site requirements) will be considered and matched to the disaster recovery requirements of the school.

Security strategies will be discussed with Pembrokeshire County Council where appropriate. The school will work with Pembrokeshire County Council to ensure e-safety and integrity of any wireless system used or installed in school.

Personal data sent over the internet will be encrypted or otherwise secured. Portable media may not be used without a virus check. Portable media must not be used to store or transfer unencrypted personal data about pupils/students or staff.

Unapproved system utilities and executable files will not be allowed in staff or pupils/students' work areas or attached to email. Students must not download copyright material – for example film, photographs or music files to the school network.

Files held on the school's network may be checked at any time in order to ensure compliance.

The ICT co-ordinator / Network Manager will review system capacity regularly.

3.2. How will email be managed?

Pupils/students may only use their approved school Gmail email accounts within school.

Pupils/students must immediately tell a teacher if they receive offensive email.

Pupils/students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

Access in school to external personal email accounts may be blocked. Excessive social email use can interfere with learning and may 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. The forwarding of chain letters is not permitted.

3.3. How will published content be managed?

The contact details on the school website should be the school address, email and telephone number. Staff or pupils/students' personal information must not be published. Email addresses should be published carefully, to avoid spam harvesting.

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

3.4. Can pupil/student's images or work be published?

Images that include pupils/students will be selected carefully. Associated texts should not enable individual pupils/students to be clearly identified. Pupils/students' names will not be used anywhere in association with photographs on the website. Written permission from parents/carers or carers will be obtained before images of pupils/students are electronically published; parents/carers must sign to opt in to give permission – consent cannot be assumed.

3.5. How will social networking and personal publishing be managed?

The school will block / filter access to social networking sites. Inappropriate forums (such as Newsgroups) will be blocked.

Pupils/students 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, IM and email addresses, full names of friends, specific interests and clubs etc.

School staff must abide by the School Staff Electronic Communication and Social Media Policy. Teachers' official blogs or wikis should be password protected and run from the school website. Teachers will be advised not to run social network spaces for student use on a personal basis.

Pupils/students will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.

Pupils/students will be advised on security and encouraged to set passwords - for example: deny access to unknown individuals and block unwanted communications; invite known friends only and deny access to others; not publish specific and detailed private thoughts.

The school deals with cyber bullying that impacts directly on school life, and assists any victims of cyber bullying to report these issues to appropriate authorities.

3.6. How will filtering be managed?

The school will work with all stakeholders to ensure that systems to protect staff, pupils/students are regularly reviewed and improved. If staff or pupils/students discover unsuitable sites, the URL must be reported to the e-safety officer and forwarded to the Network Manager immediately for the site to be added to the filtering block list.

All internet access in the school will be logged. Internet use will be randomly monitored to ensure compliance with school policy. All internet access in the school is filtered. In rare circumstances, there is a valid need to overcome technical limitations through the use of an unfiltered connection. The head teacher should personally authorise all unfiltered Internet users, and review the need for access regularly.

The school's e-safety policy ties in closely with the disciplinary policy for both staff and students. Senior staff may make random checks to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal will be reported to appropriate agencies.

3.7. How will video conferencing be managed?

Video conferencing is provided via Google Meet or Microsoft Teams. Pupils have access to this functionality disabled by default and only have it enabled when it is educationally necessary. Staff have access to these applications continually in order for it to aid them in distance learning, CPD training and sharing of good practice with other schools.

Video conferencing contact information should not be put on the school website.

Users:
Pupils/students should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing should be supervised appropriately for the pupils/students' age.

Content:
If third-party materials are to be included, staff must check that recording is acceptable to avoid infringing the third-party intellectual property rights.

Staff must engage in dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

3.8. How can emerging technologies be managed?

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

Students' mobile phones must not be used during lessons or formal school time without the express permission of staff. The sending of abusive or inappropriate text messages is forbidden.

The school will explore emerging technologies and develop policy on use in school when there are clear educational benefits.

Staff will be issued with a school phone where contact with pupils/students is required.

3.9. How should personal data be protected?

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (DPA 2018) and GDPR guidance. Details are given in the school's data protection policy.

4. Miscellaneous Policy Issues

4.1. How will internet access be authorised?

The school will maintain a current record of all staff and pupils/students who are granted access to the school's electronic communications.

All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resources.

Under the schools' statutory task of providing education, all pupils are granted internet access. Pupils/students will be educated on the schools e-safety rules and acceptable use policy as part of their ICT lessons. Failure to comply with the safety rules and acceptable use policy will result in the pupil/student's internet access being revoked.

4.2. 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. Neither the school nor Pembrokeshire County Council can accept liability for the material accessed, or any consequences resulting from internet use.

The school will review ICT use and any e-safety incidents 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.

4.3. How will e-safety complaints be handled?

Pupils/students and parents/carers should use the normal complaints procedure for complaints relating to systems and procedures. If a complaint relates to an incident where a pupil/student was at risk of harm, this could instead be reported to child protection procedures if appropriate.

Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher.

Parents/carers and pupils/students will need to work in partnership with staff to resolve issues. Discussions will be held with the Police Public Protection Unit to establish procedures for handling potentially illegal issues. Sanctions within the school discipline policy include: interview/counselling by the head of year; informing parents/carers or carers; removal of Internet or computer access for a period.

4.4. How is the internet used across the community?

The school will liaise with local organisations to establish a common approach to e-safety.

The school will be sensitive to internet related issues experienced by pupils/students out of school, e.g. social networking sites and offer appropriate advice.

4.5. Communications Policy

4.5.1. How will the policy be introduced to pupils/students?

Pupils/students will be informed that network and internet use will be monitored.

E-safety advice will be included in the PSE or ICT programmes covering both school and home use.

The school will make e-safety advice published by the local authority available to parents/carers.

4.5.2. How will the policy be discussed with staff?

All staff will be given the school e-safety policy and its application and importance explained. Staff should be aware that internet traffic can be monitored and traced and that high standards of professional conduct are expected.

Staff training in safe and responsible internet use and on the school e-safety policy will be provided to any staff who are unsure of the standards required.

Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Staff will be invited to comment on the e-safety policy prior to annual review by the governing body. The same consultation will extend to the school council.