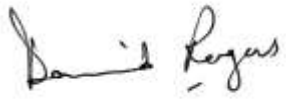
WELSHPOOL HIGH SCHOOL

E-SAFETY POLICY

DATE REVIEWED; June 2021

DATE FOR REVIEW; June 2022



SIGNED_____ Date: 10/5/21

Chair of Governing Body

10/5/21

SIGNED_____ Date:

HeadTeacher

WELSHPOOL HIGH SCHOOL

E-SAFETY POLICY

1.0 Rationale

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present. We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education.

2.0 Implementation of the policy

The senior leadership team at Welshpool High School will ensure all members of school staff are made aware of the contents of the school eSafety policy and the use of any new technology within school.

eSafety will be taught as part of the curriculum in an age-appropriate way to all pupils and suitable posters will be prominently displayed around the school. The eSafety policy will be made available to parents, carers and others via the school website. All pupils will be aware of the requirements of our Digital Access Acceptable Use Policy.

3.0 Responsibilities of the School Community

At Welshpool High School, we believe that eSafety is the responsibility of the whole school and that everyone has their part to play in ensuring all members of our school are able to benefit from the opportunities that technology provides for learning and teaching.

The following responsibilities demonstrate how each member of the community will contribute.

3.1 The Senior Leadership Team

The Senior Leadership Team (SLT) accepts the following responsibilities:

The Head Teacher will take ultimate responsibility for the eSafety of the school community. The Head Teacher will also identify a person (the eSafety lead) to take day to day responsibility for eSafety; provide them with training; monitor and support them in their work (Deborah Smith).

The SLT will ensure that adequate technical support is in place to maintain a secure ICT system and that policy and procedures are in place to ensure the integrity of the school's information and data assets. They will liaise with the Governors and develop and promote an eSafety culture within the school community.

The SLT will ensure that all pupils agree to the Digital Access Acceptable Use Policy and that new staff have eSafety included as part of their induction procedures. They will make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to eSafety

The SLT will also receive and regularly review eSafety incident logs; ensure that the correct procedures are followed should an eSafety incident occur in school and review incidents to see if further action is required

3.2 The eSafety Lead

The eSafety Lead is responsible for promoting an awareness and commitment to eSafety throughout the school; they will be the first point of contact in school on all eSafety matters and take day to day responsibility for eSafety within the school. The eSafety Lead will also be responsible for liaising with technical staff on eSafety issues.

The eSafety Lead is also responsible for creating and maintaining eSafety policies and procedures. The eSafety Lead will ensure that they develop an understanding of current eSafety issues, guidance and appropriate legislation.

The eSafety Lead will also ensure that:

- eSafety training is delivered
- eSafety education is embedded across the curriculum
- eSafety is promoted to parents and carers via the school website, Twitter and at school open evenings, parents' evenings etc
- any person who is not a member of school staff, who makes use of the school ICT equipment in any context, is made aware of the Digital Access Acceptable Use Policy
- Heads of Year will log eSafety incidents
- staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an eSafety incident
- the school eSafety policy and Digital Access Acceptable Use Policies are reviewed in accordance with the review schedule.

The eSafety Lead will also be responsible for liaising with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate. They will promote the positive use of modern technologies and the internet.

3.3 Responsibilities of all Staff

All Welshpool High School staff should read, understand and help promote the school's eSafety policies and guidance. They should also ensure that they read, understand and adhere to the Social Media guidance for Staff.

Staff should take responsibility for ensuring the safety of sensitive school data and information and where possible they should develop and maintain an awareness of current eSafety issues, legislation and guidance relevant to their work.

Staff are expected to maintain a professional level of conduct in their personal use of technology at all times. They should ensure that all digital communication with pupils is on a professional level and only through school based systems (see Social Media Policy for Staff).

Where possible, staff should endeavor to embed eSafety messages in learning activities where appropriate and ensure that they supervise pupils carefully when engaged in learning activities involving technology. Staff should ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable or is inappropriate. Any eSafety incidents which occur should be reported in the appropriate log and/or to their line manager.

3.4 Specific Teaching Staff

Deborah Smith (Head of ICT and Vocational), is responsible for embedding eSafety into the Key Stage 3 ICT curriculum and monitoring its delivery by Key Stage 3 ICT staff. eSafety guidance and information may also be delivered during PSE lessons or assemblies. Deborah Smith will also liaise with the Assistant Head Teacher with responsibility for Key Stage 3, to ensure that lower school pupils receive 'top up' training in eSafety on an annual basis; she will also provide displays, the eSafety Group board and posters relating to eSafety.

Natalie Forsyth (NF) – Assistant Head Teacher is responsible for enhancing the existing delivery of eSafety with relevant assemblies in lower school. She will also supplement school delivery of eSafety with visits from the local police during assemblies or PSE lessons. NF will also have overall responsibility for working with Heads of Year to help promote eSafety to all Lower School pupils.

Jamie Loxam (JL) – Assistant Head Teacher is responsible for enhancing the existing delivery of eSafety with relevant assemblies in upper school. He will also supplement school delivery of eSafety with visits from the local police during assemblies or PSE lessons. JL will also have overall responsibility for working with Heads of Year to help promote eSafety to all Upper School pupils.

3.5 Technical Staff

Technical Staff should support the school in providing a safe technical infrastructure to support learning and teaching. They should ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information and review these regularly to ensure they are up to date. They should ensure that provision exists for misuse detection and malicious attack. On request from the appropriate staff (e.g., the eSafety lead and/or senior leadership team), they should conduct occasional checks on files, folders, email and other digital content to ensure that the Digital Access Acceptable Use Policy is being followed.

Technical staff should report any eSafety-related issues that come to their attention to the eSafety lead and/or senior leadership team. They should ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management.

Where situations arise and there are any external users of the schools ICT equipment, it is the responsibility of the technical staff to ensure that suitable access arrangements are in place.

Technical staff should ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a serious incident or disaster.

3.6 Pupils

All pupils should read, understand and adhere to the Digital Access Acceptable Use Policy and follow all safe practice guidance. Pupils should read and understand the Welshpool High School Live Streaming Home School Agreement which covers acceptable use of the live streaming applications used via the HWB platform. Pupils should take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school. Pupils should ensure that they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home. They should understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening. Pupils should report all eSafety incidents to appropriate members of staff and discuss eSafety issues with family and friends in an open and honest way.

All pupils should know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices and school policies regarding acceptable use (see Digital Access Acceptable Use Policy and Welshpool High School Live Streaming Home School Agreement).

3.6 Parents and Carers

It is the responsibility of all Parents and Carers to help and support the school in promoting eSafety. They should:

- read, understand and promote the pupil Digital Access Acceptable Use Policy and Welshpool High School Live Streaming Home School Agreement with their children. They should also sign the Digital Data Consent and Additional Services Consent for HWB and Google Classroom which forms part of the policy. The Welshpool High School Live Streaming Home School Agreement should also be signed digitally using the link https://forms.office.com/Pages/ResponsePage.aspx?id=bHaxPS31j0SMnhTEvxPPtvCIQtl0mgRNiXRdK-FxFLFUNUpFWkozQzFFRkdJRjJETDE3WlpZSUdRRy4u

- discuss eSafety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology

- consult with the school if they have any concerns about their child's use of technology

- ensure they inform the school if they disagree with the school using photographic and video images of pupils

3.8 Governing Body

The Governing Body as a whole will read, understand, contribute to, review and help promote the school's eSafety policies and guidance as part of the school's overarching Safeguarding procedures.

The Governing Body should support the work of the school in promoting safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety

awareness. They will have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data. Finally, the Governing Body should ensure appropriate funding and resources are available for the school to implement their eSafety strategy.

3.9 Child Protection Officer

It is the responsibility of the Child Protection Officer to understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information. The Child Protection Officer should be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, cyberbullying and others.

The Child Protection Officer is responsible for raising awareness of the particular issues which may arise for vulnerable pupils in the school's approach to eSafety ensuring that staff know the correct child protection procedures to follow.

4.0 TIMELINE FOR ESAFETY TRAINING

As part of the eSafety training delivered, pupils will be given information about Cyberbullying and Responsible Social Networking.

	AUTUMN TERMS		**SPRING TERM**		**SUMMER TERM**	
YEAR 7	Internet Safety	ICT lessons	Safer Internet Day	Year Group Assembly & PSE	Internet Safety	Enquiry Day Year Group Assembly or PSE
YEAR 8	Internet Safety Cyberbullying Presentation	ICT lessons Year Group Assembly	Police Safety Talk	Year Group Assembly Or PSE	Internet Safety	Enquiry Day Year Group Assembly or PSE
YEAR 9	Internet Safety Cyberbullying Presentation	ICT lessons Year Group Assembly	Police Safety Talk	Year Group Assembly Or PSE	Internet Safety	Enquiry Day Year Group Assembly or PSE
Year 10	-	-	Safer Internet Day	Year Group Assembly & PSE	-	-
Year 11	Internet Safety Presentation	Year Group Assembly	Safer Internet Day	Year Group Assembly & PSE	-	-
Sixth Form	-	-	Responsible Social Networking Presentation	Year Group Assembly	-	-

5.0 DIGITAL ACCESS ACCEPTABLE USE POLICY

School has a Digital Access Acceptable Use Policy for all pupils. This is shared with all pupils when they fill in their admission form for the school and they will be expected to agree to it and follow its guidelines.

We will ensure that external groups and visitors to school who use our ICT facilities are made aware of the appropriate Digital Access Acceptable Use Policy. They will be required to read and sign the Digital Access Acceptable Use Policy before being allowed access to school facilities.

6.0 WELSHPOOL HIGH SCHOOL LIVE STREAMING HOME SCHOOL AGREEMENT

School has a Welshpool High School Live Streaming Home School Agreement for all pupils. This is shared with electronically via HWB email to all pupils and they will be expected to agree to it and follow its guidelines. This agreement covers live streaming of lessons via Microsoft Teams and Google Meet and the storing of personal data/data sharing.

7.0 LEARNING AND TEACHING

We will deliver a planned and progressive scheme of work to teach eSafety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. We believe that learning about eSafety should be embedded across the curriculum and also taught in specific lessons such as in ICT and PSE.

We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach plagiarism rules or copyright laws.

We will discuss, remind or raise relevant eSafety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind pupils about the responsibilities to which they have agreed through the Digital Access Acceptable Use Policy. Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

8.0 HOW PARENTS AND CARERS WILL BE INVOLVED

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will offer opportunities for finding out more information through the school website. Twitter will be used as a platform to promote eSafety resources, news and information. We request our parents to support the school in applying the eSafety Policy and the Digital Access Acceptable Use Policy.

9.0 MANAGING AND SAFEGUARDING IT SYSTEMS

The school will ensure that access to the school IT system is as safe and secure as reasonably possible. Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate.

A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff. We do not allow anyone except technical staff or the Head of ICT to download and install software onto the network.

9.1 Filtering Internet access

Web filtering of internet content is provided by Powys County Council. This ensures that all reasonable precautions are taken to prevent access to illegal content. However it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in pupils in monitoring their own internet activity.

All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However deliberate access of inappropriate or illegal material will be treated as a serious breach of the Digital Access Acceptable Use Policy and appropriate sanctions taken.

Teachers are encouraged to check out websites they wish to use prior to lessons for the suitability of content.

9.2 Access to school systems

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorizing and protecting login and password information.

9.3 Passwords

We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system). A warning is issued to all users on login.

We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school. All pupils have a unique, individually-named user account and password for access to IT equipment and information systems available within school.

All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.

The school maintains a log of all accesses by users and of their activities while using the system in order to track any eSafety incidents.

9.4 Using the Internet

We provide the internet to:

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with Powys County Council, the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

Pupils and staff are informed about the actions to take if inappropriate material is discovered:

- Staff should report to eSafety Lead and/or Head Teacher
- Pupils should report to eSafety Lead/Head of Year/Teacher

10.0 ONLINE CONTENT

10.1 School Website

The school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number.

Identities of pupils are protected at all times. Group photographs published on the school website with lists of names will not specifically identify an individual pupil.

10.2 School Twitter/Departmental Twitter/Instagram Accounts

The school uses Twitter to celebrate achievement and share relevant information. The school maintains editorial responsibility for any school initiated publishing via Twitter to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school Twitter account by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

Identities of pupils are protected at all times. Group photographs published on the school Twitter will generally list First Names only. Other departmental school related social media accounts also come under this guidance.

10.3 Creating online content as part of the curriculum

Any content created as part of the school curriculum will only be published via the school website or via the school VLE/HWB. Any exceptional circumstances required permission from the Head Teacher.

10.4 Online material published outside the school

Pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

10.5 Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

Parents receive information about taking and publishing photographs and video of their children (in publications and on website/social media). This information includes the publication of pupils' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and possibly on the website.

Any parents who do not wish to consent are invited to contact the school; their child is then added to the No Publicity List. This list is checked whenever an activity is being photographed or filmed.

10.6 Using mobile phones

During lesson time we expect all mobile phones belonging to pupils are to be switched off unless there is a specific agreement for this not to be the case.

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another pupil or staff member we do not consider it a defense that the activity took place outside school hours.

The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress, 'cyberbullying', will be considered a disciplinary matter.

We make it clear to staff, pupils and parents that the Head Teacher has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

10.7 Using mobile devices

We recognise that the multimedia and communication facilities provided by mobile devices (e.g. iPad, iPod, tablet, netbook, Smart phones) can provide beneficial opportunities for pupils. However their use in lesson time will be with permission from the Teacher and within clearly defined boundaries. If these are used then pupils are taught to use them responsibly.

Staff are encouraged to not use their own personal mobile devices to photograph/record pupils or their work, which may be required for assessment purposes or to provide evidence for examination board criteria. I-Pads and a school camera are available to staff if photo/video evidence is required.

10.8 Using other technologies

As a school we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an eSafety point of view.

We will regularly review the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

10.9 Dealing with eSafety Incidents

All eSafety incidents are recorded in the School eSafety Log which is regularly reviewed.

Any incidents where pupils do not follow the Digital Access Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious eSafety incident, concerning pupils or staff, they will inform the eSafety Lead, their line manager or head Teacher who will then respond in the most appropriate manner.

Instances of cyberbullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation to support the victim.

10.10 Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the Welshpool High School Child Protection and Safeguarding Policy apply.

10.11 Dealing with complaints and breaches of conduct by pupils:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- The school will ensure that support is offered to the victims
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies