e-Safety Policy

Ysgol Uwchradd Llanidloes High School

Status	Version 1
Policy Author	Daniel Owen
Date of Issue	12.10.2022
Date of Review	27.09.2023
Agreed by	Governing Body
Next Review Date	Autumn 2024
Authorisation	Chair of Governing Body Date: 27.09.2023 Signature:

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 leadership team at Llanidloes High School will ensure that all members of school staff are made aware of the contents of the school's e-Safety policy.

e-Safety will be taught as part of the curriculum in an age-appropriate way to all pupils. The e-Safety 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 Llanidloes High School, we believe that e-Safety 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 Headteacher will identify a person (the e-Safety lead) to take day to day responsibility for e-Safety. This person will be responsible for identifying and accessing suitable training opportunities that will enable them to carry out their role effectively.

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 e-Safety 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 e-Safety 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 e-Safety.

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

3.2 The e-Safety Lead

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

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

The e-Safety Lead will also ensure that:

- e-Safety training is delivered
- e-Safety education is embedded across the curriculum
- e-Safety 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 e-Safety 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 e-Safety incident
- the school's e-Safety Policy and Digital Access Acceptable Use Policy are reviewed in accordance with the review schedule.

The e-Safety Lead will also be responsible for liaising with the Local Authority, the (Local) Mid and West Wales 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 Llanidloes High School staff should read, understand and help promote the school's e-Safety policy and guidance. They should also ensure that they read, understand and adhere to the Social Media Policy 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 e-Safety 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 the Social Media Policy for Staff).

Where possible, staff should endeavor to embed e-Safety 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 e-Safety incidents which occur should be reported in the appropriate log and/or to their line manager.

3.4 Specific Teaching Staff

Emma Pafrey (Learning Manager for Technology), Joseph Higgs (ICT teacher) and Duncan Mason (DCF lead) are responsible for embedding e-Safety into the ICT curriculum in Years 7 to 9. Emma Palfrey is responsible for monitoring its delivery by ICT staff. e-Safety guidance and information may also be delivered during PSE lessons or assemblies. Emma Palfrey will also liaise with the Senior Link with responsibility for safeguarding, to ensure that lower school pupils receive 'top up' training in e-Safety on an annual basis; she may also provide displays relating to e-Safety.

Richard Williams (RW) (Assistant Headteacher) is responsible for enhancing the existing delivery of e-Safety with relevant assemblies. He will also supplement school delivery of e-Safety with visits from the local police during assemblies or PSE lessons. RW will also have overall responsibility for working with Heads of Year to help promote e-Safety across the school community.

3.5 Technical Staff

Technical Staff should support the school in providing a safe technical infrastructure to support learning and teaching. They should ensure that 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.

Technical staff should report any e-Safety-related issues that come to their attention to the e-Safety lead on the SLT. These will be considered by the SLT and a suitable response determined. 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 Llanidloes 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 school. Pupils should ensure that they respect the 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 e-Safety incidents to appropriate members of staff and discuss e-Safety 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 Llanidloes High School Live Streaming Home School Agreement).

3.7 Parents and Carers

It is the responsibility of all parents and carers to help and support the school in promoting e-Safety. They should:

- read, understand and promote the pupil Digital Access Acceptable Use Policy and Llanidloes High School Live Streaming Home School Agreement with their children. They should also sign the Digital Data Consent and Additional Services Consent for Hwb which forms part of the policy. The Llanidloes High School Live Streaming Home School Agreement should also be signed digitally
- discuss e-Safety 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 e-Safety awareness. They will have an overview of how the school's 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 that appropriate funding and resources are available for the school to implement their e-Safety 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 e-Safety training

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

	AUTUMN TERM		SPRING TERM		SUMMER TERM	
Y 7	Internet Safety: https://hwb.gov.wales/playlists/view/d1e004dd-12ab-4998-a664-3a4d6d2b2048/en/9	ICT lessons	Safer Internet Day	Year Group Assembly & PSE	Internet Safety	Enquiry Day Year Group Assembly or PSE
Y 8	Internet Safety Cyberbullying : https://hwb.gov.wales/playlists/view/d1e004dd-12ab-4998-a664-3a4d6d2b2048/en/10	ICT lessons	Police Safety Talk	Year Group Assembly or PSE	Internet Safety	Enquiry Day Year Group Assembly or PSE
Y 9	Internet Safety Cyberbullying: https://hwb.gov.wales/playlists/view/d1e004dd-12ab-4998-a664-3a4d6d2b2048/en/11	ICT lessons	Police Safety Talk	Year Group Assembly or PSE	Internet Safety	Enquiry Day Year Group Assembly or PSE
Y 10	-	-	Safer Internet Day	Year Group Assembly & PSE	-	-
Y 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

The 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 Llanidloes High School Live Streaming Home School Agreement

Llanidloes High School has a Live Streaming Home School Agreement (see below) for all pupils. This is shared with pupils electronically via Hwb email and they are 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 and data sharing.

7.0 Learning and Teaching

We will deliver a planned and progressive scheme of work to teach e-Safety 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 e-Safety 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.

We will discuss, remind or raise relevant e-Safety 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. Other platforms may be used to promote e-Safety resources, news and information. We ask our parents to support the school in applying the e-Safety 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 (the IT technician and Headteacher). 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). 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 e-Safety 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 e-Safety Lead and/or Headteacher
- Pupils should report to e-Safety Lead, Head of Year or Teacher

10.0 Online Content

10.0 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.

10.1 School X (Twitter), Departmental X (Twitter) and Instagram Accounts

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

GDPR guidance and regulations are followed with respect to pupil and staff privacy.

10.2 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 or Hwb. Any exceptional circumstances require permission from the Headteacher.

10.3 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.

10.4 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 taken and published in accordance with GDPR. Consent is sought wherever required. Images and videos are of appropriate activities and are only taken of pupils wearing appropriate dress.

When GDPR provides parents/pupils with the right to withhold consent, they are invited to contact the school. Where applicable, the child is then added to the No Publicity List. This list is checked whenever an activity is being photographed or filmed.

10.5 Using Mobile Phones

Students in Years 7 to 11 are not allowed to use SMART phones on the school site.

During lesson time, we expect all mobile phones belonging to sixth form pupils 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 Headteacher has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

10.6 Using Mobile Devices That Are Not SMART Phones

We recognise that the multimedia and communication facilities provided by mobile devices (e.g. iPad, iPod, tablet, netbook) 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 seek permission from senior staff or the e-Safety lead if they want to use their own personal mobile devices to photograph or record pupils or their work. This may be required for assessment purposes or to provide evidence for examination board criteria. iPads and a school camera are available to staff if photographic or video evidence is required.

10.7 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 e-Safety point of view.

We will regularly review the e-Safety 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.

10.8 Dealing with e-Safety Incidents

All e-Safety incidents are recorded using the behaviour management recording system.

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 e-Safety incident, concerning pupils or staff, they will inform the e-Safety Lead, their line manager or Headteacher who will then respond in an appropriate manner.

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

10.9 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 Llanidloes High School Child Protection and Safeguarding Policy apply.

10.10 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 Pastoral Managers or 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

LLANIDLOES HIGH SCHOOL – ACCEPTABLE USE POLICY

This acceptable use policy covers acceptable use of the Llanidloes High School network and the Hwb platform. Remember, anything you do on Hwb should have an educational purpose. You should not regard any of your activity as private or confidential. In addition to these rules you must comply with the terms and conditions for use of Hwb (see school website - documents page). You must also always keep another local copy of your essential work that you store on the cloud.

Pupils are responsible on the internet just as they are in the classroom or in a corridor. General school rules apply. The Acceptable Use Policy applies at all times, in and out of school hours, whilst using school equipment.

Protect the school community by reporting anything you see that might cause upset or harm to yourself, other teachers or learners in the school. You are expected to demonstrate a professional approach and respect for learners and their families and for colleagues and the school while online. Where staff feel they are being pestered by pupils, this may constitute a disciplinary matter. Where fellow pupils feel they are being targeted online, this may constitute a disciplinary matter.

Passwords. Keep your username and password safe. Using others' passwords is prohibited. You are responsible for anything that happens under your account. Report to your network/HWB administrator if you suspect that your username and password have been compromised. Trespassing in others' folders, work or files is prohibited.

The internet is provided for pupils to conduct research and communicate with others. Remember that access is a privilege, not a right and that access requires responsibility. This includes access via your desktop or via mobile devices. All internet access is filtered but it is important to recognise that filtering is not infallible.

Staff may monitor student's computer sessions and may review files to ensure that users are using the system responsibly. Users should not expect that files stored on servers or discs will always be private. Users should be aware that all Internet requests are logged and are ultimately traceable back to the individual user. If you share external links within Hwb then you deem that the content of the external website is age appropriate and has an educational purpose, e.g. YouTube. You may not access, distribute or place material on Hwb that is in breach of the statutory rights of copyright owners.

Emails are also monitored and can be reviewed and should be for school use only. In Hwb, personal use of your mailbox and cloud storage is to be avoided.

Using mobile technologies and your responsibilities. Be a positive role model in how you use digital technologies in including Hwb. Videos, images or recordings made in school using mobile phones, iPads, tablets, cameras or other devices, should not be posted online (this includes Facebook, Twitter, Instagram, Snapchat, YouTube etc) without permission from senior staff (e.g. when images are for publicity purposes and adhere to GDPR stipulations).

When using school Wi-Fi/Internet, users should be aware that requests are logged and are ultimately traceable back to the individual device. Attempting to access unauthorised websites using the Wi-Fi/Internet system may constitute a disciplinary matter. In addition, the following are all prohibited; creation or transmission of any unreasonably offensive, obscene or indecent images, data or other material; harassing, insulting and/or attacking others and using obscene language; using the network for gambling or commercial purposes. Content relating to or supporting illegal activities may be reported to the authorities.

I HAVE READ THROUGH, UNDERSTAND THE ACCEPTABLE USE POLICY. I HAVE DISCUSSED THE POLICY WITH MY CHILD AND AGREE TO THEM HAVING INTERNET ACCESS THROUGH THE SCHOOL NETWORK, WI-FI/INTERNET SYSTEMS AND THE HWB PLATFORM.

*

Signed: ……………………………………………………………………………….. **Date:** …………………………………….

LLANIDLOES HIGH SCHOOL – DIGITAL DATA CONSENT

STUDENT WORK AND PHOTOGRAPHS/VIDEOS/AUDIO. Work and/or photographs / videos /audio may be displayed and/or electronically published or shared for purposes such as celebration of achievement, development and training using Lesson Box and/or exemplar material. These may be stored for a period of time and disposed of securely once they are no longer required. You need to sign to give permission for Llanidloes High School to use of any still or moving images, photographs and/or frames and/or audio footage depicting your child for these purposes.

* **I GIVE PERMISSION / DO NOT GIVE PERMISSION** (delete as appropriate) ⟵ **THIS SECTION MUST BE COMPLETED OTHERWISE THE FORM WILL BE RETURNED**

* **Signed:** ………………………………………………………………………… **Date:** …………………………………

STORING PERSONAL DATA / DATA SHARING. Personal data, once collected, may be stored securely for a given period of time. Confidential information (including **personal data/photographs/videos etc.**) will be destroyed and **disposed** of **securely once** it is **no longer required.** In order to provide your child with a secure log-in, the school may send basic information to educational providers such as MathsWatch, GCSEPod, Duo Lingo, ArcGIS and Reading Cloud; this list is not exhaustive and could change during the year.

I HAVE READ AND UNDERSTAND THE STORAGE / SHARING OF PERSONAL DATA

* **Signed:** ………………………………………………………………………… **Date:** …………………………………

Hwb

HWB ADDITIONAL SERVICES CONSENT

The Hwb platform provides all maintained schools in Wales with access to a wide range of centrally-funded, bilingual digital tools and resources to support the digital transformation of classroom practices. The Hwb platform is managed and operated by the Welsh Government.

All learners in maintained schools in Wales must be provided with a secure log-in to the Hwb platform. This is because mandatory reading and numeracy tests, currently on paper, will be moving online and must be completed by each pupil via the platform.

In order to provide you/your child with a secure log-in, the school will be sending basic information to the Welsh Government. The log-in will allow you/your child to take the mandatory online assessments, known as 'personalised assessments'. For more information about the Hwb platform and how information about you/your child is used, please see school website documents section. For more information about the online personalised assessments, please see WHS website, documents section.

Additional services. If you agree, Welsh Government can also provide you/your child with access, via the Hwb platform, to a variety of additional services which are provided by other organisations. These include online learning environments such as Hwb Classes, Microsoft Office 365, Google for Education, and other relevant educational tools and resources. Welsh Government is making these additional services available to help you/your child to access educational resources. These additional services are centrally funded and there is no cost for you or for your school to access and use them.

WELSH GOVERNMENT WILL ONLY PROVIDE ACCESS TO THESE ADDITIONAL SERVICES IF YOU SIGN THE FORM BELOW TO INDICATE YOUR AGREEMENT

✓ We will tell Welsh Government to provide access to the additional services

✓ Welsh Government will share information about you/your child with its service providers, including Microsoft and Google Education, in order to enable access to the additional services.

* **Signed:** …………………………………………………………………………..……… **Date:** …………………………………….

If you wish to withdraw your consent at any time to network access, Hwb access, digital data and/or Hwb additional services, please contact the headteacher at Llanidloes High School. If you do not agree, we will still share information about you/your child with Welsh Government to set up a secure log-in for Hwb.