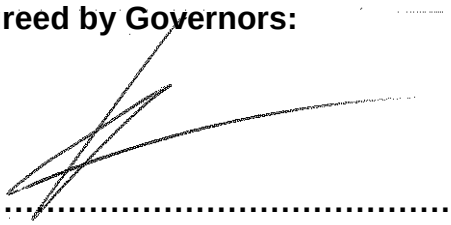
ICT Acceptable Use Policy

Agreed by Governors:



……

(Signed by Chair)

June 2019

Scheme due for review

June 2020

If you would like a copy of this document in an alternative format or your own language, please contact:

Argoed High School

Tel: 01352 756414

Email: contact@argoedhs.co.uk

Contents

Introduction and Principles

The Acceptable Use Policy is to ensure that the students of Argoed High School can use the internet, email and other school technologies, safely and securely allowing them to fully utilise the technology to achieve their true potential. The policy also covers other school technology facilities such as printers, consumables, virtual learning environments, monitoring, remote access, and many more.

The policy is designed to not only keep students and staff safe but to also protect the school network and the data it holds. Access to many sites is restricted along with reduced usage of computer settings to minimise the possibility of damage to the infrastructure, hardware and online attacks.

Argoed High School recognises the importance of ICT in education and the needs of the students to access the school facilities both inside and outside of lesson times. To allow for this we require all staff and students to sign an Acceptable Use Agreement before they can receive their school account logon details.

1. **Equipment -**

   Vandalism is defined as any action which harms or damages any equipment or data which is part of the schools facilities. Such damage is covered by the Computer Misuse Act 1990. This includes but is not limited to:

   - Deliberate damage to hardware such as monitors, keyboards, mice, base units, printers, cabling, or other hardware.
   - Change or removal of software.
   - Unauthorised configuration or setting changes.
   - Creation, deployment or uploading of computer viruses, malware or any software designed to cause harm.
   - Deliberate deletion of files or data.

   Such actions will reduce the provision available for all students and put other user's data at risk, these actions will lead to increased repairs by the IT department. This increased workload reduces the department's ability to support the schools ICT provisions as well as incurring additional costs which reduce available funds for the improvement of the school facilities. Any deliberate damage to school facilities which incur costs will result in those costs being passed to the parent or carer of the student who caused the damage.

2. **Data Storage –**

   School data is stored in various locations within the internal Flintshire network, by external suppliers and by government agencies.
   All school data stored within the Argoed High School building and within the Flintshire ICT data centres, are stored on secure servers which are updated regularly to comply with GDPR and the Data Protection Act. Severe restrictions are applied to the data to restrict user access to this data dependant on their job role and requirements; only authorised personnel have access to the data and those personnel will only have access to the data required to complete their daily duties.

   The school uses a handful of specially selected third party suppliers to help it provide the best possible service to staff, students and parents/carers. These suppliers are vetted and monitored to ensure they only have data they require to complete their tasks and that the data is stored securely and deleted when appropriate. All suppliers must comply with GDPR and the Data Protection Act and a list of these suppliers and the data they hold is available from the school upon request.

Government departments also collect school data for the use of statistical analysis. Most of the data they collect is anonymous. Any data they collect is stored securely and complies with the relevant government policies and will comply with all laws.

3. **Internet Access –**

The internet is a fundamental part of ICT provision at Argoed High School. It is available to all school staff, students and visitors with various restrictions and levels of access. All school internet access is monitored, recorded and filtered, at multiple levels. Software is used to dynamically filter students web access to remove any illegal, inappropriate or offensive content. While it is impossible to remove all this content the systems are continuously monitored and updated inline with Welsh Government guidelines.

Any use deemed inappropriate by school staff during a students use of the internet will result in that student's internet or computer access being withdrawn for an appropriate amount of time.

4. **Wireless Devices –**

The school uses many wireless devices to enhance the learning of its students and productivity of its staff. Access to the wireless networks are restricted and access is only authorised by the IT Manager. The school curriculum networks (CurricISE, CurricApple) are only authorised for school owned devices and any attempt to gain unauthorised access to them will result in appropriate sanctions. The school curriculum networks operate on the same standards, monitoring and web filtering applied to wired school computers and the same sanctions will be applied for its misuse.

The Student Guest wireless network is available for staff and student personal devices to gain internet access. All staff are provided with this access automatically while students will be allowed access to this network based on the head teacher's discretion. Students do not have automatic access to this network. The Student Guest network has advanced web filtering designed to protect the school network from potentially harmful external devices.

The Public Guest network is provided to visitors who request internet access while visiting the school and has substantial web filtering to protect the school network from potentially harmful unknown devices.

5. **Removable Storage –**

Staff
The use of removable storage is discouraged for school staff due to its unreliability and potential to cause harm to the network if not used appropriately. All staff are provided with secure cloud storage space where they should store any school related data. The use of removable storage is allowed for school staff where there is a legitimate reason for not using the school cloud storage or where the data being stored is not directly governed by the school.

Students
Students are not authorised to use any removable storage in the school computers. They are provided with the same secure cloud storage as staff and are taught how to use it. If there is a valid reason for a student to connect a removable storage device to a school computer they must first seek the permission of the IT Manager and the device will be accessed under their supervision.

6. **Email and Electronic Communications –**

   All staff and students are provided with free access to Office365 which includes Microsoft Teams, Outlook Email and OneDrive cloud storage among others. Access to this service is governed by this policy and any use of this service deemed inappropriate or not for educational use will result in access to this service being removed. Staff and students must not use their email addresses for anything other than school related communications, and the cloud storage must be only used to storage school or work-related data. Where communications or data are deemed to be of non-school use they will be removed from the system and appropriate actions will be taken where required.

7. **Downloading of Files -**

   While the school internet connection has a much greater capacity than the standard home broadband, there is still a need to be mindful that the downloading and storage of large files may impact other users. Any files downloaded onto the school network from any source must be educational or work related. The schools data is regularly checked to ensure no harmful files are being stored. Scripts, executable files, games, and other not educational or potentially harmful files are removed automatically by our systems on a regular basis and their owners and locations recorded to assist in any sanctions where clear damage or intent to cause damage is found.

8. **Web Filtering –**

   The school uses multiple layers of web filtering to protect students and staff from the potentially harmful or inappropriate areas of the internet. The primary source of filtering takes place directly through our internet line via dedicated council run servers. The filtering provided by these servers meets government regulations and is constantly updated to ensure that sites which are not appropriate are blacklisted and access to the removed for the relevant groups. The second level of filtering is done on the school premises by dedicated classroom management software. This level of filtering is much more targeted than the first as it has the ability to search for key words or phrases in the URL, web page and source code of the sites. While it is not possible to filter out all inappropriate content on the internet, our internal filtering system is constantly monitored by IT staff and any sites which appear to have become available are rapidly removed and their content blocked. Online games are not allowed on school computers and their access is heavily restricted. School computers, even during break and lunch times are to be used for school related/educational work only and users caught playing games will be asked to leave the computer room and their internet history will be screened and any unblocked sites will be checked and blocked where required.

9. **Printing –**

   Printers and photocopiers are provided throughout the school for anyone to use at any time. These devices while very efficient must be used only when required for educational purposes to keep the schools printing costs to a minimum and allow the facilities to be updated regularly. Students must take their time and proof read all work before printing to ensure printing multiple copies with small revisions is kept to a minimum.

   All printer and copier use is recorded and monitored constantly therefore if you use the devices for non-educational use or offensive use you will be subject to the schools behaviour management measures and your access to the printing devices or computers removed or heavily restricted.

10. Remote Access –

To maximise the efficiency and productivity of the IT department remote access software is installed on every school device. This allows the IT department to view a live feed of every device in the school as well as view all active windows and website history. This level of access is required to ensure IT staff and teachers can quickly rectify any problems on the end users device as well as to prevent any further damage being caused to a device. IT staff and teachers have the ability to remotely control, log off and shutdown student devices to ensure behaviour and security standards are met. IT staff may take control of a student or staff device without their prior consent where a serious malfunction of software, security event or where the IT staff see a problem which needs immediate action.

Remote access from outside the school network is heavily restricted and can only be authorised and monitored by the IT Manager. Only third party suppliers will be granted this level of access and only in cases where its not practical for school IT staff to complete the tasks under the third party's instruction. Staff and students have no access to any data stored on the school site or council servers from home.

11. External Services –

To provide the students with the best possible education we use a handful of specially selected third party suppliers to provide additional services which the school itself could not replicate effectively. Suppliers include but are not limited to: Microsoft, School Cloud Systems, Google, Apple, Impero, Hwb, Capita.

Hwb – Hwb is a Welsh Government system which is provided free of charge to every school in Wales. By agreeing to this policy, you are also agreeing to the Hwb acceptable use agreement (Appendix 1 and 2).

12. Password Security –

School students and staff passwords are chosen by the IT department to meet or exceed the relevant security protocols applied by school systems and our third party suppliers. Your school passwords are unique and solely for your eyes only. Your password must never be shared with anyone in school or out of school. If you feel your password may have been compromised you must inform your teacher or the IT department immediately and request for it to be changed across all relevant accounts.

13. Sanctions –

Sanctions will occur for staff or students where inappropriate, dangerous or damaging behaviour has occurred, the sanctions may include but are not limited to:

- Removal of access to one or more systems including, printing, email, internet, computers
- Costs incurred by the school to repair damage being passed onto parents/carers of the student which caused the damage.
- Sanctions in line with the school behaviour policy.

14. Emerging Technologies –

The school is continuously investing in emerging technologies where there is a clear and documented case of educational benefits. All relevant new technology is researched by the IT department and the school will conduct further research into cost etc, where there is deemed to be clear benefits. All new technologies brought into the school must meet the schools strict security and data protection standards.

15. Policy Monitoring and Review –

Due to the constantly changing state of technology this policy will be reviewed annually to ensure it stays relevant. Small changes may be made at any time to incorporate and new technologies or systems brought into school throughout the year.

Appendix 1: Acceptable use agreement for Hwb – template

Remember, anything you do on Hwb should have an educational purpose. You should not regard any of your activity as private or confidential.

- Be a positive role model in how you use digital technologies including Hwb.
- Keep your username and password safe. You are responsible for anything that happens under your account. Report to your Hwb administrator if you suspect that your username and password have been compromised.
- 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.
- 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.
- Creation or transmission of any offensive, obscene or indecent images, data or other material is prohibited. Content relating to or supporting illegal activities may be reported to the authorities.
- Personal use of your mailbox and cloud storage is to be avoided. E-mails may be monitored.
- Comply with the terms and conditions for use of Hwb.
- Always keep another local copy of your essential work that you store on the cloud.

Unacceptable use within Hwb (as highlighted but not limited to that above) might result in actions taken in line with your organisation's Disciplinary Policy.

Appendix 2: Consent form to allow learners access to additional services – template

Hwb additional services consent form

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 login 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 learner via the platform. In order to provide [you/your child] with a secure login, the school will be sending basic information to the Welsh Government. The login 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 https://hwb.gov.wales/privacy.

For more information about the online personalised assessments, please see http://learning.gov.wales/resources/collections/national-reading-and-numeracy-tests?lang=en#collection-2

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] 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.

Your agreement

If you agree:

- 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.

If you do not agree, we will still share information about [you/your child] with Welsh Government to set up a secure login for the Hwb platform, but [you/your child] will not be able to access the additional services.

If you wish to withdraw your consent, please contact the headteacher within [you/your child's] school.