WALES HIGH SCHOOL ACADEMY TRUST

ACCEPTABLE USE POLICY FOR ALL STAFF AND GOVERNORS USING THE ICT SYSTEMS

REVISION DATE	APPROVED BY	DATE OF APPROVAL
October 2017	Governing Body	12 December 2017
October 2019	Governing Body	8 October 2019
January 2023	Governing Body	7 February 2023 (amended July 2025)

To be reviewed every three years

All policies are available on the school website

Acceptable Use Policy for all Staff and Governors Using the ICT Systems at Wales High School

The following statements are a guideline for all staff and governors at Wales High School and must be adhered to at all times when using the school's ICT equipment and services. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school ICT equipment at other locations such as your home. Internet activity and network usage is monitored constantly for staff and student safety.

Action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies, you may be subject to disciplinary action in line with the school's established disciplinary procedures.

- Any use of school ICT systems will be for professional purposes as agreed by the school SLT.
- Remote access to the school's systems must be kept confidential and details not to be given out to anyone.
- Use of AI: You will not input sensitive school data when using AI systems. Any data that is inputted into AI language models may be freely accessible by others and data could be used by those systems. You will not submit any data on students, staff members, financial data or any other information that is deemed sensitive and private.
- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you log out when not actively using the ICT systems.
- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material, you should follow your school's procedure and report this immediately.
- You should not use any of the school's systems in an inappropriate manner. You should not attempt to gain access to areas of the school network that you do not have permissions for. You should not install any malicious hardware or software.
- You should not attempt to view or use any websites that promote piracy or illegal broadcasts of copyrighted media (i.e. online streaming of films and audio files that are protected by copyright laws).
- Any still or video images of pupils and staff (e.g. proms, school trips etc.) should be for professional purposes only. They should be taken, where practicable, using school equipment, and stored and used on site. Such images should not be taken off site without permission and a valid reason. Personal equipment may only be used with the express permission of the Headteacher (or his Senior Leadership Team representatives). Any images taken on personal equipment should be transferred to the school server at the earliest opportunity and then deleted from personal storage immediately.
- Ensure that any files on removable media (e.g. USB drives, CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Head teacher.

- All staff and governor email accounts will be enforced to enable multi factor authentication (2FA) when out of school, set up by a mobile device, in order to maximize security levels for the school's MIS, Office 365/Onedrive and email system.

- All staff are provided with an encrypted data USB to store work related data. Where staff or governors wish to use a personal storage device for work purposes, these must be encrypted before accessing the school's network.

- Any electronic communications should be related to school work only and should be through school e-mail addresses or other school systems (e.g. learning platforms). Any communication with pupils whether by email, messaging, calling or social networking must be in a professional and work-related capacity. In the interests of safeguarding protocols, you will not contact pupils for non-work/school related matters.

- Staff and student email messages from external sources containing attachments are routinely scanned and approved/denied manually by the ICT Team for malicious activities. Known exploitable file types are blocked from transmission within the WHS Domain.

- You must be vigilant when accessing email messages. Messages containing viruses, malware or suspicious links to other websites must be deleted immediately. If you do not know the sender, do not open the email, do not reply and check with ICT Support for validation.

- Any online activity, including messages sent and posts made on websites, and including activity outside of school, should not bring your professional role or the name of the school into disrepute.

- You must not use the school systems or storage areas for your own personal data. *(photos, music and video).* File storage is for work related items only.

- You should not reveal access to the staff wi-fi network to any students.

- You will not give out your personal details, or the personal details of other users, to students or parents or on the Internet. In particular, you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents.

- You should ensure that any personal or sensitive information you use or access (e.g. Bromcom or Go4Schools data, assessment data) is kept secure and used appropriately.

- You should not attempt to alter student's work in any way. Access to student folders should be done so in a professional and appropriate manner.

- Personal or sensitive information should only be taken off-site if agreed with the Head teacher, and steps should be taken to ensure such data is secure.

- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.

- You should support and promote the school Online Safety Policy and promote and model safe and responsible behaviour in pupils when using ICT to support learning and teaching.

I have read and agree to abide by the acceptable use of ICT guidelines for Wales High School

Signed: _____ Date _____

Print name: _____