Article 28: You have the right to a good quality education. You should be encouraged to go to the highest level you can.

Article 29: Your education should help you develop your talents and abilities. It should also help you learn to live peacefully, protect the environment and respect other people.

Blaenymaes Primary School

Acceptable Use Policy - Staff and Volunteers

Approved by Governing Body on	October 2024
Signed by Chair of Governors: A. Charles	
Signed by Head Teacher : KLecrass	
To be reviewed annually	October 2025

Today, new technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. These technologies can stimulate discussion, promote creativity and make learning more effective. They also bring opportunities for staff to make learning more engaging and data management more efficient. However, the school is aware that improper use of these systems could expose both the school and the user to potential legal liability. The school will endeavour to ensure that staff and volunteers have good access to ICT to enhance their work and the learning opportunities for pupils in their care. In return, the school expects staff and volunteers to agree to be responsible users of ICT.

This Acceptable Use Policy is intended to ensure that:

- staff and volunteers will be responsible users of ICT and stay safe while using the internet and other communication technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk in their use of ICT in their everyday work.

For my professional and personal safety I understand that:

- the school can monitor my use of the ICT systems, email and other digital communications;
- the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, hwb, seesaw, class dojo) outside the school and technologies owned by staff and volunteers, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players etc).

Passwords

- always use your own personal passwords to access computer based services;
- make sure you enter your personal passwords each time you log on. Do not include passwords in any automated logon procedures;
- change your password whenever there is any indication of possible system or password compromise;
- do not record your passwords or encryption keys on paper or in an unsecured file;
- only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else;
- ensure that all personal passwords that have been disclosed are changed once the requirement is finished;
- make sure that logged-on workstations are not left unattended.

Remote Access

- You are responsible for all activity via your remote access facility
- only use equipment with an appropriate level of security for remote access;
- to prevent unauthorised access to school systems, do not disclose your username and password to anyone;
- select passwords that are not easily guessed e.g. do not use your house or telephone number or choose consecutive or repeated numbers;
- avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is;

- protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- store all removable media securely;
- securely dispose of removable media that may hold personal data;
- encrypt all files containing personal, sensitive, confidential or classified data;
- ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

School ICT Equipment

- as a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you;
- ensure that all ICT equipment that you use is kept physically secure;
- it is imperative that you save your data on a frequent basis to the school's network drive (hwb) You are responsible for the backup and restoration of any of your data that is not held on the school's network drive;
- personal or sensitive data should not be stored on the desktop of laptops / PCs.
- privately owned ICT equipment may be used on guest wifi log in for school use e.g PPA
- on termination of employment, resignation or transfer, return all ICT equipment to your manager. You must also provide details of all your system logons so that they can be disabled;
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, mobile and smart phones are familiar to children outside of school too. Emerging technologies will be examined for educational benefit and the risk assessed before their use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during break and lunch times. Members of staff are not allowed (unless arranged via headteacher / SLT see below) to contact a parent/carer pupil using their own personal device.

Teachers may use personal mobile phone/device to access class dojo for communication between school and parent/carers (**please see class dojo policy).** Teachers will only respond during class time if it is an emergency, other messages will be replied to at break times or at the end of the school day.

This technology may be used for additional purposes, as mutually agreed with the Headteacher such as 'whats app communication'. The school is not responsible for the loss, damage or theft of any personal mobile device.

Any images or sound recordings made on these devices of any member of the school community should be uploaded to class dojo / twitter / hob / school website etc and then deleted from device. Written consent should always be checked before uploading photos to these platforms.

Class teachers may use these devices to upload photos as mentioned above, other staff should not use their mobile devices (unless agreed with Head teacher e.g Forest school) and use a class iPad for recording and taking photos of pupils on activities.

Users bringing personal devices into school must ensure there is no illegal content on the device.

Staff must not use these devices for personal use, while they are working with or supervising pupils (i.e. while on duty, working within class or a group).

School Provided Mobile Devices (including phones)

See above

Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Guidance for staff on the use of Social Networks & Blogs

Social networking sites (e.g. Facebook, Instagram etc) and blogging sites (e.g. Blogger, Twitter) are a way of life for many young people and adults. However, adults working with children should review their use of social networks as they take on professional responsibilities.

Once published online, information such as photographs and blogs are almost impossible to control. Some adults have been "caught out" by posting comments or remarks about work or colleagues, or inappropriate photographs.

It is advised that you make no reference to your school life on these sites to avoid bringing the school into disrepute.

EWC advice is as follows

Think before you post, comment on, or join anything online.

Act responsibly:

- what you share reflects on you, your employer, and your profession
- be aware others can share, screenshot, and copy your posts
- protect your professional reputation, think about your online image

Take care whom or what you associate with online:

- protect your personal data and information, be cautious what you share
- do not accept friend requests or follows from learners/young people, or share any personal contact data
- Do not accept friend requests from parents of pupils (exceptions maybe friendships outside of school - but be cautious)
- do not discuss learners, young people, parents, colleagues, management, or your place of work on online forums / social media sites.

1.

Don't be complacent:

- use privacy and security settings on your online social media accounts, and check these regularly
- do not share passwords or devices

Posting on social media must be kept outside of work hours (unless posting on school twitter account) this includes when absent from work.

If the school or any member of our community is placed in a difficult or upsetting situation, then the school will have no choice but to follow our Disciplinary Procedures Policy.