# INTERNET ACCESS AND E-SAFETY POLICY 2024

This document contains the specific policy and associated information relating to internet access and e safety at Pencoed Comprehensive School including the Pencoed 6th Form Centre.

Document Owner and Approval

Pencoed Comprehensive School is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff on the shared drive – Policies and Risk Assessments – policies.

Signature: Date:

Due for Review March 2026

**Change History Record**

| Version | Description of Change | Date of Policy Release |
|---|---|---|
| 1 | Initial Issue ( Complete Revision) | March 2024 |
| 2 | | |
| 3 | | |

Responsible Staff Member: EJ
Approved by Governing Body:
To be reviewed: March 2026

# Contents

# Section 1: Rationale and Aims

1.1 The purpose of Internet access and e-safety policy in our school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use supports our delivery of Curriculum for Wales, L2 and L3 qualification and is a necessary learning and administrative tool for staff and pupils.

1.2 The aims of the policy are to:

- encourage compliant use of the Internet by staff and pupils
- enhance the use of new technologies in the classroom so as to improve standards of teaching and learning
- enable research to take place into a wide range of resources and information
- develop pupils' skills in analysis and evaluation of information
- enhance pupils' digital learning skills to equip them for lifelong learning.
- allow staff to access relevant cloud based services that provide access to management information systems such as Classcharts, My Concern. SIMs etc.

# Section 2: Accessing the Internet

2.1 Internet access is supported and maintained by the local authority. It includes filtering for all users. The school has a range of computer suites and computers used by staff and pupils including over 700 Chromebooks. All staff are provided with a laptop for school work and all pupils in the Pencoed 6th Form Centre are able to loan a Chromebook for the duration of their studies. Acceptable Use policies are in place for use of Laptops by staff and loan of Chromebooks to 6th Form users. In addition parents/carers and students must sign and agree to our Internet Access and E-mail use agreement

2.2 Pupils are given clear objectives for Internet use and advice on when they may use their mobile phones or computer tablets in class for an explicit educational purpose. Use of mobile phones and tablets is not permitted on the school site except when directed in the classroom. Pupils are not allowed to record or film other pupils or members of staff unless they have consent to do so using school equipment. In the case of a member of staff, the pupil must have the verbal permission of the member of staff being photographed or filmed.

2.3 The school makes use of the Welsh Government's Hwb VLE to provide an appropriate online environment for staff and learners.

2.4 Pupils are:

- advised on e-safety in lessons and in Assemblies;
- made aware that the writer of an e-mail or the author of a webpage might not be the person they claim to be;
- encouraged to tell a member of staff immediately if they encounter any material on the Internet that makes them feel uncomfortable;
- taught ways to validate information before accepting that it is necessarily accurate;
- taught to acknowledge the source of information, when using Internet material for their own use
- advised to only use their HWB email for educational purposes.

2.5 Newsgroups and blogs can only be used by pupils for educational purposes under the supervision of teachers or teaching assistants.

2.6 Pupils and their parents/carers are asked to sign an Internet use agreement as part of their home school agreement.

2.7 All school PCs, including staff laptops used away from the school site are protected by a comprehensive security system from Sophos, this allows the school to implement security policy changes and settings that can be pushed out to devices wherever they are located.

2.8 Both BCBC and HWB have systems in place that monitor internet and user security in real time.

2.9 All users of the internet facilities at Pencoed Comprehensive will be expected to abide by the following expectations:

- Access must only be made via users' authorised account and password, which must not be made available to any other person. Users must not attempt to gain unauthorised access to any computer systems, network, data or resources.
- All internet use should be appropriate to staff's professional activity, or a student's education.
- The creation or distribution of any images, sounds, messages, or other materials, which are obscene, harassing, racist, inflammatory, malicious, fraudulent or libellous, is not acceptable.
- Activity that may be considered unethical, immoral, or illegal, threatens the integrity of the school's ICT systems or reputation, or that attacks or corrupts other systems, will be seen as a serious breach of school rules.
- Sites and materials accessed must be appropriate to school work. Users will recognise materials that are inappropriate, and should expect to have their access removed.
- Users are responsible for emails they send, and for contacts made that may result in emails being received. Sending messages that may annoy other people, interfere with the work of others, or result in the person receiving them losing their work or systems is not acceptable.
- Professional levels of language and content should be used at all times when communicating via email, particularly as email is often forwarded.
- Posting anonymous messages and forwarding chain letters is not allowed.
- Copyright materials and intellectual property rights must be respected.
- Use for personal financial gain, gambling, any form of campaigning, political purposes, or advertising is forbidden.

## Section 3: The School Website

3.1 The Headteacher delegates editorial responsibility to a member of staff to ensure that the content of the school website is accurate and quality of presentation is maintained.

3.2 The website must comply with the school's guidelines for safeguarding

3.3 All material published must either be the author's own work, or permission to reproduce it must be obtained and clearly marked with the copyright owner’s name.

3.4 The point of contact for any material on the school website is the school with the address and telephone number displayed.

3.5 Home information or individual e-mail identities must not published.

3.6 Photographs must not identify individual pupils unless parental permission has been obtained.

3.7 Full names are not used on the website without parental permission.

## Section 4: Using the Internet in the classroom

4.1 Hwb is accessed through the internet is necessary for delivery of the curriculum.

4.2 In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school supervises pupils and takes all reasonable precautions to ensure that they only access appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a computer or handheld device used in school. Neither Pencoed Comprehensive School nor the Bridgend Local Authority accepts liability for the material accessed by pupils, or any resulting consequences.

4.3 The use of the school's computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990

# Section 5: E Safety

5.1 Pupils are informed that their Internet use may be monitored. The school works in partnership with parents, the local authority, Welsh Government and the school's Internet Service Provider, the LA to ensure methods of identifying, assessing and minimising risks are kept under review and improved to protect pupils.

5.2 Actions taken include:

- maintaining access through HWB emails and learning platform
- Making use of Multi Factor verification away from the school site
- Filtering of internet and emails by BCBC
- posting rules for responsible internet use near computer systems;
- providing all staff including teachers, supply staff, teaching assistants and support staff with this Internet Access and E-Safety Policy;
- giving parents access to the policy via the school website;
- reporting any unsuitable sites discovered by staff or pupils to the Internet Service Provider via the Network Manager – giving both the URL (address) and the nature of the content;
- referring any suspected illegal material to the local authority Audit Department and the Internet Watch Foundation;
- using appropriate filtering to protect against inappropriate materials;
- discussing security strategies with the local authority;
- keeping under review the security of the whole system with regard to threats posed by hacking or Internet viruses;
- encrypting personal data sent over the Internet where appropriate;
- installing and regularly updating virus protection.

# Section 6 Cyber Security

6.1 If the school loses access to data, a backup and restoration plan is in place to mitigate against Cyber Security incidents as well as other business recovery incidents such as fire, floods, physical damage or failure or theft. Backups are kept segregated from the school's network and are tested with regard to restoration.

6.2 Cyber Security is referenced in relevant school policies and procedures e.g. business continuity plans.

6.3 The Network Manager provides regular updates to staff on matters relating to Cyber Security such as the protocols relating to the use of USB sticks, password management and the use of dual factor authentication, being aware of phishing e-mails etc.

6.4 School Cyber Resilience is discussed in meetings and the school makes use of latest Sophos Anti-Virus software.

# Section 7 Other Issues

7.1 Complaints. Any complaints or concerns about the use of the Internet should be raised using the procedure set out in the school's complaints policy. Complaints of a child protection nature must be dealt with in accordance with school Child Protection procedures and should be raised with the Designated Safeguarding Lead.

7.2 Misuse including use of AI (Artificial Intelligence).

Any misuse of the internet by pupils is dealt with in accordance with the school's Pupil Behaviour policy.

Students who misuse AI such that the work they submit for assessment is not their own will have committed malpractice, in accordance with JCQ regulations, and may attract severe sanctions. For further clarification, review: JCQ – AI USE in Assessments Documentation

7.3 Information. Relevant sources of information on safe Internet use by children and young people include:

- The Child Exploitation & Online Protection Centre - internet safety - https://www.ceop.police.uk/safety-centre/
- NCH Action for Children A Parents' Guide to the Internet, leaflet http://www.nchafc.org.uk/internet/
- Internet Watch Foundation http://www.iwf.org.uk Centre for Technology in Education
- Report Remove | Childline www.childline.org.uk
- NSPCC Report and Remove Nude images https://www.nspcc.org.uk

## Section 8 Review

8.1 The policy itself will be reviewed every 2 years unless changes are needed at an earlier stage.

## Section 9 Related policies and documents

- Data Protection policy
- Child Protection and Safeguarding policy
- Social Media Use for Staff policy
- CCTV policy