Cardiff Steiner School

Student IT Acceptable Use Policy (AUP)

Prepared with reference to:

- Data Protection Act 1988 (and Amendment Act 2003)
- GDPR (General Data Protection Regulation)
- Welsh Government 'Respecting others: Cyberbullying/ Guidance document No: 057/2011
- Welsh Government Circular 23/03: 'Respecting Others: Anti Bullying Guidance'
- Hwb Online Safety https://hwb.gov.wales/zones/online-safety/
- All Wales Child Protection Procedures 2008
- Welsh Assembly Government Safeguarding Children; working together under the Children Act 2004
- Welsh Assembly Government Keeping Learners Safe

Contents

1. Strategy and Overview

The aim of this Internet Acceptable Use Policy (AUP) is to ensure that digital learners at Cardiff Steiner School benefit fully from the learning, teaching and assessment opportunities offered by our School's internet and intranet resources in a safe, effective and accountable manner.

Internet use and access is considered a resource and privilege. Cardiff Steiner School benefits from a modern high speed broadband fibre based connection, accessible through networked PCs and Wi-Fi system. Users must be aware that their bandwidth usage may affect access speeds and quality of service for other users.

If our school's AUP is not adhered to, internet use and access may be withdrawn from users and appropriate actions taken, as per our school's 'Behaviour Policy Lower School and Upper School'.

When using the internet students are expected:

- to access appropriate areas of learning
- to treat all others with respect at all times
- to respect the right to privacy of all members of our school community
  to understand copyright and acknowledge creators when using online content and resources
- not to undertake any actions that may bring Cardiff Steiner School or any members of the school community into disrepute

This AUP applies to all students who access the internet at Cardiff Steiner School or use the school's digital platforms outside of School.

Misuse of the internet that impacts on the well-being of students and/or staff under this policy and associated Behaviour and Anti-Bullying Policies, may result in disciplinary action, including verbal warnings and contact with parent(s)/guardian(s), withdrawal of access privileges, and when necessary, exclusion from the School. Cardiff Steiner School also exercises the right to report any illegal activities to the appropriate authorities.

The following strategies promote safer use of the internet:

- Students will be provided with support and instruction in internet safety as part the curriculum.
- Cardiff Steiner School may participates in Safer Internet Day activities which aim to promote safe and effective use of the internet.
- E-Safety School webpage

The implementation of this Student Internet Acceptable Use Policy will be monitored by all staff.

The School will monitor the impact of the policy using surveys of students, parents, and staff as appropriate.

2. Content Filtering

Cardiff Steiner School implements content filtering on the Schools Broadband Network (SBN). This is CIPA compliant. Cardiff Steiner School reserves the right to use additional filtering policies on network Service Set Identifiers (SSIDs) to ensure availability and quality of service of our available bandwidth for all users.

Students taking steps to bypass the content filter by using proxy sites or other means will be subject to disciplinary action as per the School's Behaviour Policy.

3. Web Browsing and Downloading

3.1. Students will use the School's internet connection and digital platforms only for educational and career development activities
3.2. Students will be aware that any usage, including distributing or receiving information, school-related or personal, will be monitored for unusual activity, security and/or network management reasons
3.3. Students will not download or upload materials or images not relevant to their studies
3.4. Students will not intentionally visit internet sites that contain gambling, pornographic, obscene, illegal, hateful or otherwise objectionable materials
3.5. Students will not copy information from the internet without acknowledging the creator and referencing the source of the content
3.6. Students will not engage in online activities such as updating personal devices or transferring large files that result in heavy network traffic which impairs the service for other internet users
3.7. Students will not download or view any material that is pornographic, illegal, obscene, and defamatory or that is intended to annoy or intimidate another person
3.8. Students will not promote or use virtual private networks (VPN) to hide Internet Protocol (IP) addresses

4. Email and Messaging

4.1. All school-related communications must be made using students School Google Mail account. The use of student's personal email accounts is not allowed for school purposes
4.2. Students should not share their email account username and password with others under any circumstances.
4.3. Students should not use school email accounts to register for online services such as social networking services, apps, gambling and games.
4.4. Students should not use School email accounts to register or access their online student bank accounts or other financial transactions (e.g. topping up student travel cards, mobile phone credit management, reward schemes etc.)
4.5. Student email accounts will be limited to sending and receiving mail within the *cardiffsteiner.org.uk* domain
4.6. Students will not send any material that is: pornographic, illegal, obscene, defamatory or that which is intended to annoy or intimidate another person.

4.7. Students should immediately report to their Class Teacher/Guardian or a Senior Person for Child Protection the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and under no circumstance should respond to any such communication.
4.8. Students should avoid opening emails that appear suspicious and report accordingly to their Class Teacher/Guardian
4.9. Where provided, students are expected to use email addresses issued under the *cardiffsteiner.org.uk* domain for all classwork

G-suite is used to host the *cardiffsteiner.org.uk* email service and all email sent from our domain must include the following disclaimer:

5. Social Media

5.1. Students must not use social media and the internet in any way to harass, insult, abuse or defame students, their family members, staff, or other members of the school community
5.2. Students must not discuss personal information about fellow students, staff and other members of the school community on social media
5.3. Students must not use school email addresses for setting up personal social media accounts or to communicate through such media
5.4. Students must not engage in activities involving social media which might bring the School community into disrepute.
5.5. Students must not represent their personal views as being representative of the School community on any social media platform

6. Personal Digital Devices

Students using their own digital devices in school, or to access the School's digital platforms and services at home, should follow the rules set out in this AUP, in the same way as if they were using School equipment. *Digital Devices* include smartphones, wearable technology, digital tablets, media players and any device which is or has the capability to be connected to the internet through an ethernet, WIFI, hotspot or cellular connection.

The following statements apply to the use of internet-enabled devices:

6.1. Students are only allowed to bring personal devices to School with the written and express permission of staff **and** the written permission of their parent/carer, in the form of a signed copy of the Permission Form at the end of this Policy, given to the School.
6.2. It is the responsibility of the student to ensure the safe storage of their device when not in use, e.g. during break and lunch times. The School accepts no liability for loss or damage.
6.3. Students are only allowed to use personal devices during lessons with the express permission of staff.
6.4. Students are not allowed to use personal devices outside of class time. If there are exceptional reasons for this these will be recorded, with the express permission of staff, on the Permission Form.
6.5. Students must ensure that any apps/updates are downloaded and installed before lessons to ensure they are ready for use in class and do not impact bandwidth for other users.
6.6. Devices must be brought to School charged, with a suitable screen protector and protective case
6.7. Any unauthorised capture of images, video or audio is in direct breach of the school's AUP and will be dealt with under our Behaviour and associated policies.
6.8. Digital devices must be turned off when not in use or not required for class. (devices in 'silent' or 'vibrate' mode are not considered 'off')

7. Images & Video

7.1. Students must not take, use, share, publish or distribute images of others without their permission.
7.2. Taking photos or videos on school grounds or when participating in school activities is ONLY permitted when undertaking a learning activity and only with the instruction of a teacher.
7.3. Taking photos or videos on school grounds or when participating in school activities is ONLY allowed with expressed permission from staff.
7.4. Students must not share images, videos or other content online with the intention to harm another member of the School community.

7.5. Sharing images of individuals is an unacceptable and absolutely prohibited behaviour, and will be dealt with as per the School's Behaviour Policy and associated policies.
7.6. Taking or distributing explicit, self-generated images is absolutely prohibited, and will be dealt with as per the School's Behaviour Policy, Child Protection Policies and associated policies, and will be reported to the appropriate authorities.

8. Cyberbullying

8.1. When using the internet students are expected to treat others with respect at all times.
8.2. Engaging in online activities with the intention to harm, harass, or embarrass another student or member of staff is an unacceptable and absolutely prohibited behaviour, and will be dealt with as per the School's Behaviour Policy and Anti-Bullying Policy.
8.3. Students must be aware that cyber-bullying is defined as follows "Cyber bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others." and will be dealt with, as appropriate, in line with the School's Behaviour and Anti-Bullying Policies.
8.4 Cyberbullying can include a wide range of unacceptable behaviours), and, like face-to-face bullying, cyberbullying is designed to cause distress and harm. Cyber bullying can involve emails and mobile phones used for SMS messages and as cameras, social networking sites, group apps, instant messenger and Voice over Internet Protocol, video hosting sites, and gaming sites, consoles and virtual worlds.
8.4. The prevention of cyber bullying is an integral part of the School's Anti-Bullying Policy. Students should familiarise themselves with the Anti-Bullying Policy on the School's Policies webpage

9. School Website / Social Media Platforms

9.1. Students' work and achievements will be promoted on the school website and social media platforms.
9.2. The publication of student work on the School website and social media platforms must be submitted via a member of staff.
9.3. Digital imaging and video clips showing individual students will only be published on the school website and social media platforms with parent/guardian permission.
9.4. Personal student information including students' home address and contact details will not be published.
9.5. To protect the identity of students, full names will not be used with digital content published online.

Cardiff Steiner School

AUP Permission Form

Student Agreement

I have read, understood and will follow the AUP at Cardiff Steiner School in both word and spirit to use the Internet and School's digital learning platforms in a responsible way and to maintain a safe digital environment for myself and all other members of our School community.

Student's Name _____ Class: _____

Signature: _____ Date: _____

Parent/Carer Permission

As a parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my child/the child in my care to access the Internet at School and use the School's Learning Platforms. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the School to provide for online safety but the School cannot be held responsible if students access unsuitable websites.

Please also tick the following as appropriate

- ❑ I accept that, if the School considers it appropriate, my child's work may be chosen for inclusion on the School website and social media platforms to celebrate achievement. I understand and accept the terms of the Acceptable Use Policy relating to publishing students' work.
- ❑ I agree to my child bringing a personal device to School in line with this policy (applicable only to students in Class 10 up; for students using the device to support Additional Learning Needs; or in other approved, exceptional circumstance).

Parent/Carer Name/s _____

Signature: _____ Date: _____

School Permission

I agree to the above student bringing a personal device to School in line with this policy (applicable only to Class 10 up, for students using the device to support Additional Learning Needs or in other approved, exceptional circumstance [detailed below]).

Staff Member Name _____

Signature: _____ Date: _____

Notes: _____ _____

Please review the attached school Internet Acceptable Use Policy sign and return this form to Nicola Robinson in the School Office. Parents/carers and/or the School may revoke permission at any time, and permission may be reviewed on breach of the policy.

Issue date

This policy takes effect from March 2020

Review date

This policy and its implementation will be reviewed by the School Administrator/ DSPCP as required in the light of changing technologies and relevant national and EU legislation

Review will include where appropriate the following stakeholders:

- Digital Strategy Mandate Group
- Teaching staff and College of Teachers
- Students Council
- School Management Team

Date of Next Review: March 2021

Endorsement

Full endorsement to this policy is given by:

Name: Miranda Knight

Position: School Administrative Manager /Designated Safeguarding Lead

Signed: 

Date: 26 March 2020

Related policies

This policy should be cross-referenced to related School policies including:

- Behaviour Policy Lower School and Upper School
- Anti-Bullying Policy
- Child Protection Policy and Procedures
- Data Protection Policy and Procedures
- G Suite Privacy Notice
- E-Safety for Parents webpage