CARDIFF SIXTH FORM COLLEGE

E-Safety Policy

September 2023

Document Quality Control

Original

Version	Author	Date	Reviewed By	Date
December 2016	Lisa Morton	December 2016	David Fear	March 2017

Document Reviews/Updates

Document Version Editing	Reason for Review/Update	Reviewer	Date	Checked / Approved By	Date
December 2016	Policy check and update	David Fear	March 2017	David Fear	March 2017
March 2017	Annual Review	David Fear	March 2018	Victoria Matthews	December 2018
December 2018	Document Formatting	Cerys Williamson	August 2019	Gareth Collier	Aug 2019
August 2019	Update	Lisa Morton	January 2020	Gareth Collier	January 2020
January 2020	Annual Review	Lisa Morton	September 2021	Gareth Collier	September 2021
September 2021	Annual Review	Tom Arrand	September 2022	Gareth Collier	September 2022
September 2022	Annual Review	Tom Arrand	September 2023	Gareth Collier	September 2023

Contents

Policy

1.0 Introduction

1.1 This policy should be read in conjunction with other relevant college policies to which it refers e.g. Safeguarding and Child Protection, ICT Acceptable Use, Anti-bullying, Staff Handbook, Prevent, PSE and RSE (Personal, Social Education and Relationships and Sexuality Education), Conducting a Search and Use of Physical Intervention, and the Behaviour, Rewards and Sanctions Policy.

1.2 In drafting the policy, the College has responded to guidance provided by the Welsh Assembly and national Government.

- Keeping Learners Safe, Welsh Assembly Government
- Enhancing digital resilience in education: An action plan to protect children and young people online (2020)
- Keeping Safe Online area on HWB (Including 'In the Know')
- Live streaming and video-conferencing: safeguarding principles and practice HWB
- Recommended web filtering standards for schools in Wales
- Sharing. Nudes and semi-nudes: Responding to incidents and safeguarding children and young people
- Advice for schools on preparing for and responding to viral online harmful challenges and hoaxes
- Respecting Others: Cyberbullying September 2011 (Guidance document no: 057/2011)
- Sexting: Responding to incidents and safeguarding learners: Guidance for educational settings in Wales UKCCIS
- The online safety: Five key questions for governing bodies to help challenge their schools and colleges to effectively safeguard their learners
- All Wales Practice Guide on Safeguarding children from online abuse

1.3 Cardiff Sixth Form College recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all students and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

1.4 Our approach is to implement the appropriate safeguards within the College while supporting staff and pupils to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard pupils we will do all that we can to make our pupils and staff stay e-safe and to satisfy our wider duty of care. E-safety is part of the College induction and

through PSE and RSE (Personal, Social Education and Relationships and Sexuality Education) and college assembly sessions, pupils are informed about the importance of staying safe online. In addition to this, the College accesses the Welsh Government HWB – E-Safety Zone and Keeping Safe Online area resources and these are advertised to pupils through the College's PSE and RSE sessions.

1.5 The College has also appointed a number of student leaders who look to promote E-Safety for fellow students by following E-Safety Campaigns and within college assemblies.

1.6 The College also actively promotes Safer Internet Day and the student safeguarding and wellbeing website advertises support to learners on online safety and harmful online content, the Report Harmful Content and Childline's Report and Remove Tool.

2.0 Creation, Monitoring and Review

2.1 The impact of the E-Safety Policy will be monitored regularly with a full review being carried out at least once a year by SLT, the Designated Safeguarding Person and the College IT Manager who is responsible for MIS at the College. The policy will also be reconsidered where particular concerns are raised, when government legislation or recommendations are noted; for example, via the Prevent agenda, and/or where an e-safety incident has been recorded previously in the College. This will then allow for reflective practice and for any future College practices to be appropriately reviewed in line with welfare and pastoral care.

3.0 Policy Scope

3.1 The E-safety Policy applies to all users/all students and staff/all members of the College community who have access to the College IT systems, whether on the premises or under the duty-of-care of the College.

3.2 The E-safety Policy extends to all stakeholders if and when their online conduct has an impact on the wellbeing and/or ability to learn/work of any member of the college community, or on the reputation of the college or any member of the college.

3.3 All users of College IT systems must agree to the ICT Acceptable Use Policy; which includes the e-Safety policy statements, each time they logon to the College network.

3.4 The E-safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phone, social media sites and use of images/video of the College community. In addition to this, students are asked upon enrolment to sign a student charter in which acceptable use of all IT is noted and students are required to abide by.

4.0 Roles and Responsibilities

4.1 There are clear lines of responsibility for E-safety within the College. The first point of contact should be the Designated Safeguarding Person for all concerns of breaches of internet safety.

4.2 All staff are responsible for ensuring the safety of pupils and should report any concerns immediately to the Designated Safeguarding Person. All teaching staff are required to deliver E-safety guidance when using online technology in the classroom.

Within classes, pupils will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly. In addition to this, provisions are put in place to ensure that students are aware of harmful sites and the dangers of using the internet through police talks and guest speaker sessions as part of PSE and RSE (Personal, Social Education and Relationships and Sexuality Education) and pupils are given external links that can also offer support if they have concerns about online safety or wish to learn more about how to keep themselves safe online.

4.3 The college student safeguarding and wellbeing websites contain e-safety information and helplines regarding a variety of issues and the staff safeguarding website directs college staff to useful resources, such as the Professionals Online Safety Helpline (POSH). Students and parents will also be made aware of whom they can contact if they have concerns about online safety.

4.4 All students with responsibilities are also be given key information about e-safety in order to effectively signpost those students who may be in need of advice or support, this includes online harms associated with Peer-on-Peer Abuse.

4.5 The College also has student leaders, who promote e-safety amongst the student body and frequent PSE and RSE (Personal, Social Education and Relationships and Sexuality Education) give advice and guidance to young people on how to stay safe online.

4.6 The DSP is CEOP trained and reminds staff of guidance on 'Sharing nudes and semi-nudes', ensuring that staff are aware not to forward or view any illicit images that have been disclosed to them.

4.7 College staff are aware of the main forms of child abuse via ICT: content, contact, conduct and Commerce.

4.7.1 **Content** - This refers to harm through exposure to images, text and audio that are age appropriate, offensive and illegal.

4.7.2 **Contact** - This refers to harm through interactions with others.

4.7.3 **Conduct** - This refers to harm arising from how children and young people behave when communicating themselves or with adults using ICT.

4.7.4 **Commerce** – This refers to risks such as online gambling, inappropriate advertising, phishing and or financial scams.

4.8 In addition to the abuse, staff should also be alert to risk factors which include but are not limited to:

- Virtual Identities
- Unsupervised Contact
- Online Communities
- Ease of Sharing Information
- Violent Extremism

4.9 When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. The College's Safeguarding and Child Protection Policy should be referred to and followed at all times.

4.10 Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, additional support from external agencies may be required, such as Cardiff Children's Services, the Police and CEOP (Child Exploitation and Online Protection Centre).

4.11 The E-safety (Designated Safeguarding Person) Officer is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will be expected to record incidents in line with the College's Safeguarding and Child Protection procedures and report any developments and incidents to the Principal and liaise with the local authority and external agencies to promote e-safety within the College community. The Designated Safeguarding Person will also liaise with the Designated Safeguarding Governor for additional guidance and good practice, as cited within the College Safeguarding and Child Protection Policy.

4.12 In line with the above, the Designated Safeguarding Person will make available to staff key guidance from local and national organisations involving e-safety such as 'sexting' and youth produced sexual imagery.

4.13 Any new or temporary users, such as visitors will receive a new password or temporary password and will be required to accept and agree to the College ICT Acceptable Use Policy. All staff are responsible for using College IT systems and mobile devices in accordance with the College's ICT Acceptable Use Policy and the E-safety Policy Statements. The College uses a filtering system, 'Smoothwall' across sites and all staff and students have login and a Wi-Fi log in. Staff and/or students accessing inappropriate material will be flagged to the College IT Manager and the Designated Safeguarding Person will be informed if an investigation needs to take place. Staff are responsible for displaying a model example to pupils at all times through good practice.

4.14 All digital communications with pupils must be professional at all times and be carried out in line with the College Safeguarding and Child Protection and ICT Acceptable Use Policies. Online communication with pupils is restricted to the college network only. External platforms not hosted by the college, such as social media sites, may only be used when they are linked directly to a curriculum area for educational purposes e.g. Twitter, Facebook and should not be used for the promotion of materials or personal use. All College accounts must be led by a curriculum member of staff.

4.15 This policy will, however, be monitored and kept under review, by the SLT, IT Manager, Designated Safeguarding Person, Deputy Designated Safeguarding Persons and the Designated Governor for Safeguarding.

4.16 **Students** are responsible for using the College IT systems and mobile devices in accordance with the College ICT Acceptable Use Policy and E-safety Policy Statements. Online e-safety awareness campaigns run by the student leaders and college staff aim to make pupils aware of the dangers of online usage along with an understanding of their own responsibilities in order to stay safe online. PSE and RSE sessions with Heads of Houses also make pupils aware of the issues connected to using online platforms, digital footprints and promotion on how and where support can be accessed throughout their sessions.

4.17 **Students** must act safely and responsibly at all times when using the internet and/or mobile technologies in their own time. They are expected to know and act in line with other relevant College policies. They must follow reporting procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the College community.

4.18 E-safety promotion will be widely available at the College through the pastoral team, PSE and RSE lessons, guest speakers, noticeboards, online student platforms such as the safegaurding and wellbeing websites and through the promotion of awareness days and weeks by the college Wellbeing Officer through assemblies.

4.19 **Students** are signposted to The UK Safer Internet Centre www.saferinternet.org.uk and CEOPs Thinkuknow Website – www.thinkuknow.co.uk. In addition to this the Welsh Government's HWB E-Safety Zone and Keeping safe Online area resources can be accessed for PSE and RSE sessions and students and staff are made aware of the use of social media for online radicalisation via the college safeguarding team, the Safeguarding and Child Protection Policy and the Prevent Policy.

4.20 The College's Anti-bullying and the Safeguarding and Child Protection Policy make reference to cyberbullying and the processes that need to be followed. In cases where online bullying has been found to have occurred, the college will follow procedures outlined in the Safeguarding and Child Protection Policy, along with the Anti-bullying and Rewards and Sanctions Policy.

5.0 Security

5.1 The College will do all that it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of college systems and information. Digital communications, including email and internet postings, over the College network, will be monitored in line with the ICT Policies.

6.0 Behaviour

6.1 Cardiff Sixth Form College will ensure that all users of technologies adhere to the standard of behaviour as set out in the Behaviour, Rewards & Sanctions Policy and outlined in the Staff Handbook.

6.2 The College will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and pupils should be courteous and respectful at all times.

6.3 Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with relevant policies.

6.4 Where conduct is found to be unacceptable, the College will deal with the matter internally.

6.5 Where conduct is considered illegal, the college will report the matter to the police or a relevant official external body. The flowchart in the appendix makes it clear what sanctions will be applied for specific behaviours.

7.0 Use of Images and Video

7.1 The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or pupils. The college's Data Protection Policy should be referred to at all times.

7.2 All pupils and staff receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites. For the learner this is embedded in to the pastoral programme and through promotional awareness programmes such as PSE and RSE (Personal, Social Education and Relationships and Sexuality Education), assembly slots and awareness weeks and days.

7.3 Cardiff Sixth Form College's curriculum staff and Head of House team will provide information to pupils on the appropriate use of images; this includes photographs of pupils and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe. Use of photographs of activities on the College premises should be considered carefully. Pupils sign a consent form during the application process, either allowing or withdrawing consent for the College's use of a learner's image. Approved photographs should not include names of individuals without consent. The College GDPR Champion should be consulted with any queries regarding this.

8.0 Incidents and Response

8.1 Where an e-safety incident is reported to the College, the matter will be dealt with very seriously. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to any staff member who has a duty to inform the Designated Safeguarding Person in line with the College's Safeguarding and Child Protection Policy.

8.2 Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place; external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

8.3 The e-safety incident reporting procedure flowchart in the appendix lists behaviours and their consequences. This is in line with the College's ICT Acceptable Use Policy. Serious incidents will be dealt with by the Designated Safeguarding Person and other members of SLT, in consultation with appropriate external agencies.

Appendix 1

E-Safety Policy Statements for Students

- I will not visit sites which contain items that are illegal, defamatory, pornographic or in any way offensive.
- I will observe the rules and laws regarding copyright and plagiarism.
- I will observe the requirements of the Data Protection Act 1998 and take appropriate steps to protect all personal data.
- I will report any information that I come across which makes me feel uncomfortable or unsafe to the Designated Safeguarding Person/and or Deputies.
- I agree never to write or send malicious or offensive e-mails or social media posts and accept that offenders will be reported to the Designated Safeguarding Person, the Senior Vice Principal or the Principal; depending on the severity of the incident.
- I understand that downloading and/or distributing offensive/illegal materials will lead to exclusion and possibly the involvement of the police.
- I agree to use photographs and video clips only with the specific permission of staff and students and only for educational purposes.
- I understand that if I am found to be involved in on-line bullying, that this will be dealt with in line with the College's Anti bullying policy.
- I will never give my log in details to anyone else or attempt to access the network using a log in that is not my own.
- I will never slander staff, students or the College on any social networking site, e.g. Facebook, Twitter, Snapchat, TikTok etc.

Appendix 2

E-Safety Incident Reporting Procedure Flowchart