IT Acceptable Use Policy

July 2023

Document Quality Control

Original

Version	Author	Date	Reviewed By	Date
Version 1	David Fear	May 2022	Gareth Collier	May 2022

Document Reviews/Updates

Document Version Editing	Reason for Review/Update	Reviewer	Date	Checked / Approved By	Date
May 2022	Annual Update	Julian Davies	July 2023	Chris Sweet	August 2023

Contents

1.0 Introduction

1.1 Cardiff Sixth Form College (CSFC) Cambridge prides itself on its innovative approach to the use of ICT. We are progressive in our approach and wholeheartedly encourage the sensible use of technology in all the teaching and administrative functions of the college.

1.2 This policy encompasses the following technologies, but it is not limited to:

- Websites
- Artificial Intelligence (AI)
- Email, instant messaging and chat rooms
- Social Media, including Facebook, X (formerly Twitter), Snapchat, Instagram etc.
- Mobile/ Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality
- Gaming, including online
- Learning platforms and virtual learning environments
- Blogs and wikis
- Podcasting
- Video broadcasting
- Music downloading

1.3 This policy relates to all staff, governors, visitors and students. It is inclusive of both fixed and mobile internet technologies provided by the college (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc). It includes technologies owned by students and staff, but brought onto college premises (such as laptops, mobile phones and other mobile devices).

1.4 This policy, supported by the college's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole college community. It is linked to the following mandatory college policies: Safeguarding and Child Protection, Anti-Bullying, E-Safety and Prevent. Reference is also made to the college's legal obligations such as they fall under Prevent Duty.

2.0 Data Security

2.1 CSFC Cambridge recognises that it holds potentially sensitive personal data on students and staff. Whilst the college has in recent years embraced cloud computing, the college's central database (on which is held the Single Central Register, as well as student and parent information) is stored locally. Staff and students are permitted to use their own devices in college and are periodically reminded of the importance of security and good data management.

3.0 Monitoring

3.1 Authorised ICT staff may inspect any ICT equipment owned or leased by the college at any time without prior notice.

3.2 Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving members of the college community, without consent, to the extent permitted by law. This may be to confirm or obtain college business related information; to confirm or investigate compliance with college policies, standards and procedures; to ensure the effective operation of college ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulation May 2018, or to prevent or detect crime.

3.3 Authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any college related issues retained on that account.

3.4 All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with General Data Protection Regulation May 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

3.5 Note that personal communications using college ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

4.0 Email

4.1 The use of email within CSFC Cambridge is an essential means of communication for all members of the community. Email should not be considered private. The college recognises that educationally, email can offer significant benefits including facilitating direct written contact between students and staff working on different projects. The college also recognises that students need to understand how to operate email and compose messages appropriately as part of their preparation for life beyond college.

5.0 Managing email

5.1 CSFC Cambridge gives all staff and students their own email account to use for all college business. This is to protect members of the college community and minimise the risk of receiving unsolicited or malicious emails. It also avoids the need for personal contact information to be revealed.

5.2 It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged. If necessary email histories can be traced.

5.3 Under no circumstances should staff contact students, parents or conduct any college business using personal email addresses. The college email account should be the account that is used for all college business.

5.4 The college requires a standard disclaimer to be attached to the base of all email correspondence. Emails from staff should also have the latest college-endorsed signature block attached to them.

5.5 All emails should be written and checked carefully before sending, in the same way as a letter written on college headed paper.

5.6 Staff sending emails to external organisations, parents or students are advised to cc their line manager.

5.7 College email accounts are intended for the use of the account holder only. Under no circumstances should account details be shared; nor should emails be sent from an email address by anyone other than the address owner. Sending an email from someone else's account - with or without their permission - is a serious offence.

5.8 Students may only use college approved email accounts for sending emails that are to do with the day-to-day college business. Staff should not engage in email conversations from a student who uses a non-college address.

5.9 Emails created or received as part of your work in college will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:

- Delete all emails of short-term value
- Carry out frequent housekeeping on all folders and archives
- The forwarding of chain letters is not permitted in college.

5.10 All email users are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission. Attachments should be virus checked.

5.11 Students must immediately tell a teacher or trusted adult if they receive an offensive email. Staff must inform their line manager if they receive an offensive email.

5.12 Students are introduced to email as part of the college induction process delivered by heads of house.

5.13 However members of the college community access their college email (whether directly, through web browser when away from the office or on non-college hardware) all the college email policies apply.

6.0 Sending email

6.1 When sending email containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section emailing Personal, Sensitive, Confidential or Classified Information.

6.2 Use your own college email account so that you are clearly identified as the originator of a message.

6.3 Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.

6.4 Do not send or forward attachments unnecessarily. Whenever possible share documents in Google format. Share them appropriately to save having to make multiple copies and to ensure a contemporary copy is used.

6.5 College email is not to be used for personal advertising.

7.0 Receiving email

7.1 Check your college email regularly.

7.2 Activate your 'out-of-office' notification when away for extended periods.

7.3 Never open attachments from an untrusted source.

7.4 Do not use the email system to store attachments. Detach and save business related work to the appropriate shared drive or folder.

7.5 The automatic forwarding and deletion of emails outside the domain is not allowed.

8.0 Emailing Personal, Sensitive, Confidential or Classified Information

8.1 When email must be used to transmit personal, confidential, classified or financially sensitive data to external third parties or agencies, obtain consent from your line manager to provide the information by email.

8.2 Exercise caution when sending the email and always follow these checks before releasing the email:

- Verify the details, including accurate email address, of any intended recipient of the information.
- Verify (by phoning) the details of a requestor before responding to email requests for information.
- Do not copy or forward the email to any more recipients than is absolutely necessary.

- Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone).
- Do not identify such information in the subject line of any email.
- Do request confirmation of safe receipt.

9.0 Social Media

9.1 A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chat-rooms, media posting sites, blogs and any other social space online. It includes but is not limited to, sites such as Facebook, Instagram, Snapchat, X (formerly Twitter) and Wikipedia etc.

9.2 This policy applies to the use of social media for both business and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff or students or any other IT equipment.

9.3 Staff breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to cooperate with our investigation, which may involve handing over relevant passwords and login details so far as this is consistent with the right of an individual to private and family life.

9.4 Staff or students may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

10.0 Relationship with other college policies

10.1 If an internet post would breach any of our policies in another forum it will also breach them in an online forum. For example, staff are prohibited from using social media to:

- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations they may have relating to confidentiality;
- breach our Disciplinary Rules;
- defame or disparage the college or our affiliates, parents, staff, students, business partners, suppliers, vendors or other stakeholders;
- harass or bully other staff in any way or breach our Anti-harassment and bullying policy;

- unlawfully discriminate against other staff or third parties or breach our Equal Opportunities policy;
- breach our Data Protection policy (for example, never disclose personal information about a colleague, student or parent online);
- breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

10.2 Behaviour online can be permanent and so staff and students must be extra cautious about what they say as it can be harder to retract.

10.3 Staff and students must also be aware of the particular risks to internet security that social media presents and so to comply with this policy on internet security and necessary extra measures must be taken so as to not allow any of their actions on social media sites to create vulnerability to any college systems.

10.4 Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

11.0 Responsible use of social media

11.1 Staff must be aware that their role comes with particular responsibilities and they must adhere to the college's strict approach to social media.

11.2 Staff must:

- ensure that wherever possible their privacy settings on social media sites are set so that students cannot access information relating to their personal lives;
- obtain the prior written approval of the Principal, to the wording of any personal profile which you intend to create where the college is named or mentioned on a social networking site;
- seek approval from the Principal before they speak about or make any comments on behalf of the college on the internet or through any social networking site;
- report to their Head of Department or Line Manager immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the college;
- immediately remove any internet postings which are deemed by the college to constitute a breach of this or any other college policy;
- consider whether a particular posting puts their effectiveness as a staff member at risk;
- only post what they want the world to see.

11.3 Staff must not:

- provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the college and create legal liability for both the author of the reference and the college;
- post or publish on the internet or on any social networking site, any reference to the college, your colleagues, parents or students;
- use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations;
- discuss students or colleagues or publicly criticise the college or staff;
- post images that include students;
- initiate friendships with students on any personal social network sites;
- accept students as friends on any such sites; staff must decline any student-initiated friend requests;
- use social networking sites as part of the educational process e.g. as a way of reminding students about essay titles and deadlines.

12.0 Personal use of social media

12.1 We recognise that staff may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity.

12.2 While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the organisation's business are also prohibited.

12.3 Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our IT systems. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.

13.0 The monitoring of social media

13.1 The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data,

document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

13.2 We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

13.3 We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

13.4 Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

14.0 Social media and the end of employment

14.1 If a member of staff's employment with our college should end, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that you are no longer employed or associated with our college.

14.2 All professional contacts that a member of staff has made through their course of employment with us belong to our college, regardless of whether or not the member of staff has made social media connections with them.

15.0 E-Safety

15.1 Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and that some have minimum age requirements, usually 13 years. Further information is found in the college's E-Safety Policy.

15.2 Staff are aware that some students may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues. Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these students.

16.0 E-Safety in the Curriculum

16.1 ICT and online resources are increasingly used across the curriculum. Cardiff Sixth Form College Cambridge believes it is essential for e-Safety guidance to be given to the students on a regular and meaningful basis. E-Safety is embedded within our enrolment programme and we continually look for new opportunities to promote e-Safety.

16.2 Educating students about the online risks that they may encounter outside college is done within the college PSHE programme.

16.3 Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities.

16.4 Students are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Cyberbullying is discussed through the college's PSHE programme. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, ChildLine or the CEOP report abuse button.

17.0 E-Safety Skills Development for Staff

17.1 New staff receive information on the college's acceptable use policy as part of their induction.

17.2 All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety.

17.3 All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

18.0 Managing the college e-Safety Messages

18.1 We endeavour to embed e-Safety messages across the curriculum whenever the internet or related technologies are used

18.2 The e-Safety policy is introduced to the students at the start of each college year.

19.0 Incident Reporting

19.1 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to a teacher or SMT (if you are a student) or to the Operations Manager (if you are a teacher). Similarly, all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or

unauthorised use of ICT and all other policy non-compliance must be reported to both the Operations Manager and the GDPR Champion.

20.0 Inappropriate Material

20.1 All members of the college community are made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to a teacher or line manager, as appropriate.

20.2 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Operations Manager, depending on the seriousness of the offence; investigation by the Principal, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

20.3 Users are made aware of sanctions relating to the misuse or misconduct.

21.0 Internet Use

21.1 You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

21.2 Do not reveal names of colleagues, customers or students, others or any other confidential information acquired through your job on any social networking site or blog or other online application.

21.3 On-line gambling is not allowed and the playing of non educational games is not permitted during college hours.

21.4 It is at the Principal's discretion as to what internet activities are permissible for staff and students.

21.5 The college reserves an absolute right to monitor the internet activity of all users on the network. Following the government's 2015 guidance on radicalisation, filters have been reviewed to ensure that all the words mentioned on page 5 of this government briefing document are explicitly banned.

22.0 Students' use of internet

22.1 Use of the internet, including email, is permitted as directed by the teacher for purposes of research and learning directly related to the curriculum. Outside normal college hours students are permitted to use the college's internet and their college email account for personal purposes providing that, in doing so, they do not contravene the rules and expectations laid down elsewhere in this document.

22.2 The college's internet connection is a fast1 connection. However, the bandwidth is not infinite. All users are expected to share the resource. Any use which leads to data

transfer of more than 30GB in any monthly period is deemed excessive and could result in the user's account being 'throttled' - the download speed restricted.

22.3 Students are not permitted to download any .exe file. This action is blocked by the software on the server.

22.4 The use of game-style activities should be monitored by the teacher in charge to determine suitability. Games which are not age appropriate, contain violence, inappropriate language or behaviour demeaning to others are not permitted. Students are to follow any directions relating to gaming activity from the supervising member of staff.

22.5 Accessing websites that contain content and images which are not age appropriate, i.e. from a film, television programme or game deemed to be for older viewers is not permitted. This is at the discretion of the supervising member of staff.

22.6 Images from the internet are not to be accessed, downloaded or printed without prior permission from a supervising member of staff.

22.7 Students are permitted to view videos through YouTube – many are extremely useful for learning. However, the college reserves the right to withdraw this privilege from individuals or groups if it is felt that it is being misused.

22.8 Personal email, social networking (Facebook, X (formerly Twitter) etc.) or instant messaging sites (WhatsApp, Snapchat etc.) are only to be accessed by students during college free time. There are no exceptions to this, if a member of staff has concerns regarding access to age restricted activities action may be taken to report student activity to the website provider.

22.9 Students should report any misuse of the internet to their teacher.

22.10 Students should be made aware of the possibility and consequences of online bullying.

22.11 When email is required as part of a curriculum based lesson, all emails transmitted and received will be approved by teaching staff.

22.12 No emails will be approved where they may include information that may offend others or where they do not respect the rights, beliefs and feelings of others. Students of Cardiff Sixth Form college Cambridge should always remember that they are representing themselves and our college.

22.13 Personal information such as full names, home addresses, and phone numbers will never be sent by email.

23.0 Student use of the college network

23.1 All students will be given a username to access the network. Students must log onto the college network using this username only.

24.0 Staff use of internet

24.1 Use of the internet on college premises should principally be for college use, e.g. accessing learning resources, educational websites, researching curriculum topics, use of email on college business.

24.2 Use of the college's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded.

24.3 The college recognises that information can now be accessed online through the 'streaming' of data, i.e. radio, television, music, etc. Teachers and administration staff should only be accessing streamed information if it is of educational interest to a lesson or to its planning. For example, using BBC iPlayer is acceptable if it is the interest of the class and related lessons. Streaming music for personal use is discouraged. This is due to the streaming process placing demands on the college's internet bandwidth; as a result the internet can become slow for other users.

24.4 Teachers should not be accessing the internet for personal reasons whilst teaching students.

24.5 Use of the internet to access any illegal sites or inappropriate material is a disciplinary offence. If accessed accidentally users should report the incident immediately to the Deputy Head, Pastoral or Operations Manager where it will be logged.

24.6 Staff must not access any college computer to access social networking sites, such as Facebook, X (formerly Twitter), etc., for recreational use during normal working hours. Any damage caused to college computer equipment due to accessing these sites is the responsibility of the member of staff, unless authorised by the Principal.

24.7 The college recognises that many staff will use Facebook, X (formerly Twitter), and other such social networking sites, blogging and messaging services. Staff must not post material (including text or images) which damages the reputation of the college or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other members of staff via these networks. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.

24.8 It is never acceptable to accept a 'friendship request' from students at the college. It is also extremely inadvisable to accept as friends ex-students. If a parent of a student seeks to establish contact, the member of staff should exercise their professional judgement at all times. The only exception to this is if a member of the same family attends Cardiff Sixth Form College.

24.9 All sensitive data, such as children's details and report comments, should be stored on an encrypted storage device or password protected laptop. Other data, such as lesson plans and resources, should also be stored on an encrypted devices.

24.10 Under no circumstances should staff contact students, parents or conduct any college business using their personal email addresses.

25.0 Use of mobile phones and recording devices

25.1 Whilst it is recognised that members of staff may need to use their own telephone to contact each other, or relay information regarding expected arrival times from trips etc., staff are advised that contact with parents should, wherever possible, be undertaken through the college telephone system. Parents should be discouraged from contacting members of staff on their personal mobile phones. All calls to staff regarding college business should where possible are directed through the main college telephone number. House staff have college mobile phones, as do members of the SMT.

25.2 College mobile phones are available for off-site trips and this avoids the need for staff to give out their personal mobile phone number to students or parents. If a staff member must use their own mobile phone, any student telephone numbers recorded in it must be deleted within 72 hours of the end of the trip.

25.3 Any photographs of activities including children taken on a personal device must not be shared and should be deleted or transferred to the college network as soon as possible and within 72 hours of the activity ending or the end of the trip (whichever is sooner).

25.4 Mobile phones and other cameras must never be used in an area where students or staff might change.

25.5 Mobile phones should not be used when teaching, unless in an emergency.

26.0 Use of digital images

26.1 Any photos or videos taken by teachers, other adults (including parents), and the students themselves during any college activity (including educational visits) should not be put on public display or published anywhere on the internet (including social networking websites).

26.2 The above excludes the publication of photos on the Cardiff Sixth Form College website and social media accounts, within the college magazine, for the purpose of college related publicity, and where used by the college for educational or for display uses.

27.0 Use of college hardware (laptops, cameras, recording equipment, etc.)

27.1 Use of college laptops, cameras, video cameras and recording equipment is limited to activities directly related to college activity. They can be used during lessons, sporting activities, college visits and residential trips. They are not for personal use.

27.2 All data must be transferred to the college network as soon as possible to ensure that data is saved and protected. Once copied to the network the data must be deleted from the recording equipment.

27.3 If travelling with these hardware items, and they contain information relating to staff or students, i.e. address details, photographs or reports, ensure that files are encrypted and password protected.

27.4 All members of staff will be given a username and password. Staff must log onto the college network using their personal username and password only. Staff must not access the college network using the administrator username and password unless given permission

27.5 Staff must not download software onto the college network before first liaising with the Operations Manager to check for suitability. Software that is installed and is deemed not necessary for use in the college context will be deleted.

28.0 Advice to students on Cyberbullying

28.1 Being sent an abusive or threatening text message, or seeing nasty comments about yourself on a website, can be really upsetting. This code gives you seven important tips to protect yourself and your friends from getting caught up in cyberbullying, and advice on to how to report it when it does happen.

28.2 Always respect others

- Remember that when you send a message to someone, you cannot see the impact that your words or images may have on the other person. That is why it is important to always show respect to people and be careful what you say online or what images you send. What you think is a joke may really hurt someone else. Always ask permission before you take a photo of someone.
- If you receive a rude or nasty message or picture about someone else, do not forward it. You could be assisting a bully and even be accused of cyberbullying yourself. You could also be breaking the law. The Safeguarding team, or any other member of college staff need to be informed immediately of this.

28.3 Think before you send

- It is important to think before you send any images or text about yourself or someone else by email or mobile phone, or before you post information on a website. Remember that what you send can be made public very quickly and could stay online forever. Do you really want your teacher, parents or future employer to see that photo?

28.4 Treat your password like your toothbrush

- Don't let anyone know your passwords. It is a good idea to change them on a regular basis. Choosing hard-to-guess passwords with symbols or numbers will help stop people hacking into your account and pretending to be you. Remember to only give your mobile number or personal website address to trusted friends.

28.5 Block the Bully

- Most responsible websites and services allow you to block or report someone who is behaving badly. Make use of these features, they are there for a reason!
- Don't retaliate or reply
- Replying to bullying messages, particularly in anger, is just what the bully wants.

28.6 Save the evidence

- Learn how to keep records of offending messages, pictures or online conversations. These will help you demonstrate to others what is happening and can be used by the college, internet service provider, mobile phone company, or even the police to investigate the cyberbullying.

28.7 Make sure you tell

- You have a right not to be harassed and bullied online.

28.8 There are people that can help

- Tell a member of staff you trust who can help you to report it to the right place, or call a helpline like ChildLine on 0800 1111 in confidence. Tell the provider of the service you have been bullied on (eg your mobile-phone operator or social-network provider). Check their websites to see where to report. Your teacher, guardian, House Staff or any other member of staff will support you and can discipline the person bullying you.

28.9 If you have any concerns regarding any other the above, please inform a member of college staff.

29.0 ICT Code of Conduct

29.1 The ICT facilities at Cardiff Sixth Form College Cambridge are provided: as an aid to academic work; in lessons for private study and research; and as a means of communication between staff, students, parents and others. Students are expected to use the college equipment and software for the purposes stated above. Reasonable personal use is permitted. ICT equipment owned by students and used on college premises is subject to the same terms, and must be used in accordance with our Bring Your Own Device (BYOD) Policy.

29.2 The CSFC ICT Code of Conduct must be adhered to by all staff and students:

- I know that I will be allowed to use the network and internet if I use it responsibly. I understand that if I do not, my access to the network and internet might be restricted or closed, temporarily or permanently.
- I know that the college may examine internet access histories, emails and stored files as part of routine supervision or following any suspected breach of ICT rules.
- I will not attempt to bypass network or internet controls (eg firewall).

- I will lock a computer down or log off when leaving a computer unattended, even for a short time.
- I will not share my college password(s) with any other person, nor will I impersonate another using their logon details.I will not use more data than is reasonable.
- I will not look for bad language, inappropriate images or violent games, and I know that if I accidentally come across any I should report it to a teacher or parent.
- I will never tell anyone I meet on the internet my home address, my telephone number or my college's name without permission, or send a picture of myself. I will never arrange to meet anyone in person.
- I will never hang around in a chat room if someone says or writes something which makes me feel uncomfortable or worried and I will always report it to a teacher or parent.
- I will never answer unpleasant, suggestive or bullying emails or messages and I will always report them to a member of staff. I know not to delete them straight away but show them to the person I have reported it to, as evidence.
- I will always be myself and not pretend to be anyone or anything I am not. I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I may not download any software from the internet. I know that information on the internet may not always be reliable and may need checking. I know that some websites may be sponsored by advertisers.
- I will be polite and sensible when I email others and not send, or encourage, material which may offend or annoy others or invade another person's privacy.
- I know that I am not allowed on personal email, social networking sites or instant messaging in college (during lessons).
- I will use printers for college work only and not print a very large number of copies without permission.
- I appreciate the dangers of 'sharing' machines across the network, which opens them to viruses or other contamination, and understand that sharing of licensed software, music and video is illegal.
- I will save important work in college recommended stores: my user area on the network or in my Google Drive.
- I understand that hacking of any nature or attempting to access material belonging to anyone else without specific permission is strictly prohibited.
- I will obtain permission from the Principal before publishing material concerning the college, staff or students anywhere on the worldwide web.