CAMPBELL
COLLEGE

Est 1894

DIGITAL SAFETY AND ICT ACCEPTABLE USE POLICY

Designated Staff For Digital Safety

Digital Safety Coordinator	**Mrs M Debbadi (Senior Teacher / Head of ICT)**
Network Manager	**Mr S Liggett (Network Manager)**
Designated Teacher for Child Protection	**Mr W Keown (Vice Principal)**

Revised:	**March 2025**
Next Revision:	**March 2027**

This document contains:-

1. POLICY PURPOSE

1.1 LINKS TO OTHER POLICIES 3

1.2 APPENDICES 4

1.3 ROLES AND RESPONSIBILITIES 5

1.4 PROFESSIONAL DEVELOPMENT FOR STAFF 6

1.5 SAFEGUARDING ISSUES 6

1.6 DIGITAL SAFETY EDUCATION 7

1.8 COMMUNICATION OF THIS POLICY 7

1.9 PROCESS OF REVIEW 7

2. DIGITAL DEVICES - ACCEPTABLE USE (All Users)

2.1 Passwords 8

2.2 WiFi Access 8

2.3 Internet Access via mobile devices (e.g. 3G, 4G and 5G) and personal hotspots 8

2.4 Electronic communication 8

2.5 VPN use in college 8

2.6 Virtual Learning Environments 9

2.7 Personal devices 9

2.8 Proper Use 9

2.9 The use of social media 10

2.10 Published Content 10

APPENDIX 1 ACCEPTABLE USE AGREEMENT FORMS 12

APPENDIX 2 USE OF DIGITAL CONTENT – Images etc 15

APPENDIX 3 DIGITAL SAFETY GUIDANCE FOR PARENTS 18

APPENDIX 4 GUIDANCE FOR STAFF ON DEALING WITH AN DIGITAL SAFETY INCIDENT 19

APPENDIX 5 CYBERBULLYING 20

APPENDIX 6 DIGITAL SAFETY IN BOARDING DEPARTMENT 21

APPENDIX 7 ELECTRONIC DEVICES: SEARCHING AND DELETION 22

ELECTRONIC DEVICES: SEARCHING AND DELETION 22

APPENDIX 8 CONTACTS AND RESOURCES 23

APPENDIX 9 DIGITAL SAFETY GUIDANCE FOR STAFF 24

APPENDIX 10 USE OF SOCIAL MEDIA ASSOCIATED POLICY 26

APPENDIX 11 PLAGIARISM AND USE OF ONLINE MATERIAL (Students) 27

APPENDIX 12 USE OF ARTIFICIAL INTELLIGENCE (Students) 29

1. POLICY PURPOSE

Digital Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technologies. It is an ever growing and changing area of interest and concern.
This policy applies to all members of the college community (including students, staff, volunteers, parents/guardians and visitors) who have access to and are users of the College ICT systems both in and out of the college.

Important: *This document can only be considered valid when viewed on the College VLE (Firefly) or Internet Web Page. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.*

Purposes

- To educate members of the college community regarding the safe and secure use of digital technology and applications
- To protect the college networks and equipment
- To protect the college data

Summary for Students

Key guidance points provided for students states that all students:-

- Are responsible for using the College digital technology systems in accordance with this policy,
- Should avoid plagiarism, uphold copyright regulations and ensure AI is not misused when completing assigned tasks,
- Never wilfully access or transmit inappropriate material,
- Know the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so,
- Should understand the College Policy on the use of personal digital devices,
- Should understand the College's stance on Cyber-bullying,
- Should understand the importance of adopting good Digital Safety practice when using digital technologies.

Summary for Parents

Key guidance points provided by this policy include:-

- The role of parents in ensuring Digital Safety
- Primary means for digital communication with the College (via hmoffice@campbellcollege.co.uk)
- Advice on contacting students during the school day,
- The Colleges approach to Digital Safety education,
- How students can ensure acceptable use of digital devices (school and personal),
- Consequences associated with violations of policy guidelines,
- The Colleges Digital and Acceptable Use Agreement for students,
- Details of supporting policies and guidance documents designed to ensure student safety in their use of school and personal digital devices.

1.1 POLICY PURPOSE

This Policy should be read in conjunction with the other policies of the College, including but not limited to the Safeguarding and Child ProtectionPolicy, Postive Behaviour, Addressing Bullying Policy and the Mobile Phone Policy.

1.2 APPENDICES

- **Appendix 1 - Digital Safety and Acceptable Use Agreement (for Students)**
- **Appendix 2 - Use of images and Photographs of Students**
- **Appendix 3 – Digital Safety Guidance for Parents and Staff**
- **Appendix 4 - Guidance on dealing with a Digital Safety Incident**
- **Appendix 5 - Cyberbullying**
- **Appendix 6 – Digital Safety within the Boarding Department**
- **Appendix 7 - Electronic Devices: Searching and Deletion**
- **Appendix 8 - Contacts and useful Resources**
- **Appendix 9 – Digital Safety and Acceptable Use for Staff**
- **Appendix 10 - Use of Social Media Policy**
- **Appendix 11 - Plagiarism and Use of Online Material Policy for Students**
- **Appendix 11 – Use of Generative Artificial Intelligence for Students**

1.3 ROLES AND RESPONSIBILITIES

Digital Safety Coordinator:-

- Takes day-to-day responsibility for Digital Safety issues and has a leading role in establishing and reviewing the College's Digital Safety policies, documents, and procedures.
- Ensures all staff are aware of the procedures to be followed in the event of a Digital Safety incident, and provides training and advice to staff (see Appendix 4)
- Liaises with the College's technical staff.
- Receives reports of Digital Safety incidents and keeps a log of incidents to inform future Digital Safety developments.
- Reviews curriculum resources for the promotion of Digital Safety across the curriculum delivered through in conjunction with the Head of LLW.
- Manages risk assessment on the technologies within the College.

Network Manager:-

- Ensures that the College's technical infrastructure is not open to misuse or malicious attack and meets required Digital Safety requirements and guidance issued by the Department of Education.
- Ensures that users may only access the College networks and devices is appropriately secured as per the College's Access Control policy.
- Regularly monitors the use of the network / internet / VLE / remote access and email in order that any misuse is reported to the Digital Safety Coordinator.
- Ensures that any software / systems are implemented/uploaded.

Teaching and Support Staff:-

- Be aware of current Digital Safety matters, the current Digital Safety policy and practices.
- Have read and understood this policy.
- Report any suspected misuse or problem to the relevant staff member (see Appendix 4 and Appendix 5).
- Keep any form of communications with students / parents / guardians to a professional level (and carried out using official college systems).
- Ensure they and students avoid plagiarism and uphold copyright regulations and guidance around the use of generative AI (see Appendix 11 and Appendix 12).
- In lessons which involve the use of electronic media / internet, to check the suitability of all material before the lesson.
- Outside of college hours, ensure students make appropriate use of college digital technology infrastructures (see Appendix 6).
- To ensure students know to report any unsuitable material that is found in internet searches

Students:-

- Are responsible for using the College digital technology systems in accordance with this policy.
- Should avoid plagiarism, uphold copyright regulations, and ensure AI is not misused when completing assigned tasks (see also Appendix 11 and Appendix 12).
- Never wilfully access or transmit inappropriate material.
- Know the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the College Policy on the use of personal digital devices.
- Should understand the College's stance on Cyber-bullying.
- Should understand the importance of adopting good Digital Safety practice when using digital technologies out of college and realise that the College's policy covers their actions out of college (though the College cannot police the internet when the students are in the care of their parents/guardians).

Heads of Year / Tutors:-

- Will investigate and deal with any reports of misuse / attempted misuse of the network or electronic media.
- HoYs will deal with any reports of cyberbullying (See Anti-Bullying Policy).

Safeguarding Designated Teachers

- Will investigate and deal with any incident which involves or may involve a safeguarding concern (such as access to illegal materials, the transmission or receipt of illegal images, inappropriate contact with adults/strangers, potential or actual incidents of grooming etc.).

Parents / Guardians:-

Parents play a crucial role in ensuring that their son understands the need to use digital tools appropriately, See Appendix 3 for additional guidance. We ask that parents support the College in promoting good Digital Safety at home and ensure that they and their son follow guidelines on the appropriate use of:

- Digital and video images taken at college events,
- Mobile phones and mobile devices when in college (and where this is allowed),
- Use of social media sites at home (there are barred in college),

Further information / guidance for parents can be achieved through targeted Parents Forum workshops and from Appendix 8 - Contacts and useful Resources.

1.4 PROFESSIONAL DEVELOPMENT FOR STAFF

The Digital Safety Coordinator will be responsible for coordinating the professional development of staff in e-Safety, and the Designated Teacher will brief all staff on specific Safeguarding issues.

- A planned programme of formal Digital Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Digital Safety needs of all staff will be carried out regularly.

- All new staff will receive Digital Safety training as part of their induction programme, ensuring they fully understand the college Digital Safety policy and acceptable use arrangements
  NCSC Recommended Training Programme.

- The Digital Safety Coordinator will receive regular updates through attendance at external training events when offered.

- This Digital Safety Policy will be presented to and discussed by staff in team meetings / Staff Development Days.

- The Digital Safety Coordinator will provide advice / guidance / training to individuals as required.

- Staff will be made aware that all C2k systems are monitored and that security reports can be accessed by the headmaster (or designated deputy).

1.5 SAFEGUARDING ISSUES

If College staff, parents or students suspect or are made aware of the following illegal acts it must be reported to the Designated Teacher immediately:

- A child under 16 enticed or coerced to engage in sexually explicit conduct on-line.
- Importing or transporting obscenity using telecommunications public networks.
- Knowingly receiving images of child abuse whether via the internet or other digital device (e.g. mobile phone) Images which appear to be photographs whether made by computer graphics or otherwise are also covered under Sexual Offences legislation.

The Designated Teacher will follow the procedures outlined in the Safeguarding and Child Protection Policy if such an event comes to light in college.

Appendix 2 contains the policy and permission forms for the taking, storage and use of visual images of students.

1.6 DIGITAL SAFETY EDUCATION

Digital Safety will be a focus in different areas of the curriculum and staff will reinforce Digital Safety messages across the curriculum. The Digital Safety curriculum will be provided in a number of ways:

A planned Digital Safety curriculum is provided as part of ICT and LLW lessons

- The collection of input from students (via the College Council) to inform key training and information sessions provided for students.
- Key safety messages are reinforced as part of a planned programme of tutor periods, year Assemblies and College Assemblies.
- Students are taught in lessons to be critically aware of the materials / content they access on-line.
- Students are taught to acknowledge the source of information and to respect copyright when using materials on the internet.
- Students are taught in lessons to report any inappropriate content to the class teacher.
- Students are made aware that the schools computer network is monitored, and security reports can be accessed.

We provide information and awareness to parents through:

- The provision of a Digital Safety Policy.
- College policies and advice leaflets to parents:
    - "*Digital Safety – Guidance for Parents*" available on the College website
    - "*Parents Guide to Published Pastoral Care Policies and Procedures*"

1.7 RESPONSIBILITY FOR PROPERTY

Students remain responsible for their own property and will bear the responsibility of any losses. The College cannot be held responsible for any losses incurred. Any personal electronic equipment that they bring into college must remain under their personal care and they must ensure it is stored securely and properly insured.

1.8 COMMUNICATION OF THIS POLICY

This policy will be made available to all staff, parents, and Students on FireFly and on the college website.

1.9 PROCESS OF REVIEW

This policy is reviewed annually by the ICT Department, the Safeguarding Team and the Designated Teachers for Digital Safety. The College may update this policy at any time.

2. DIGITAL DEVICES - ACCEPTABLE USE (All Users)

At Campbell College, we are delighted to offer a range of information technologies to students and staff. However, it's important to remember that access to our ICT facilities is a privilege that comes with certain responsibilities. To prevent misuse, we kindly ask students and parents to read, understand, and agree to the following terms and conditions.

2.1 Passwords

All users will be provided with a secure login for use with the Campbell College Network, students must provide a secure password on their first logon to the network. Student passwords should be something they will easily remember but it should not be obvious to other students.
Those who have forgotten their passwords or feel that the security of their passwords has been compromised should speak immediately to a member of the ICT department so their password can be reset.

Passwords should never be shared with or used by another individual.

Users will be required to update their password at least once a term. Responsibility to do this lies with the individual and failure to do so will prevent access to the College network when the password automatically expires. Reminders will be issued, and facilities provided to enable students to update passwords regularly.

2.2 WiFi Access

WiFi access is available throughout the College. The network is password protected. Any person authorised to connect to the College WiFi is bound by the terms and condition of this Policy. User logins are used to distinguish staff from guests and students. Internet access will be filtered accordingly. For this reason, staff should not ensure students do not have access to devices connected to the staff Wi-Fi network. Please note that access to the College WiFi is monitored and misuse of this resource by individuals will result in their devices being denied access to the WiFi network.

2.3 Internet Access via mobile devices (e.g. 3G, 4G and 5G) and personal hotspots

Some personal electronic devices may allow internet access or the creation of personal 'hotspots'. Students may only connect to their own hotspot, which must be password protected. They must not allow others to connect to their hotspot and will be responsible for the safety of their personal password. Students remain responsible for their electronic safety when accessing the internet via their own mobile device and must abide by the terms and conditions contained within this policy.

2.4 Electronic communication

All staff and students have a college related email account (for students this is the email address ending with @ccblearning.org.uk). All users should use this email accounts for college related business. Users should be aware that email accounts are monitored and filtered. Where an email communication is filtered incorrectly, users should seek assistance through the IT Services Team.

Electronic communication from parents to teachers should be through the college generic email account in the first instance, hmoffice@campbellcollege.co.uk. Communication through FireFly messaging may not always be 'picked-up' by classroom teachers.

2.5 VPN use in College

VPN stands for Virtual Personal Network. This is an encryption tool that offers increased security when accessing the internet. Use of VPNs is not permitted on College networks as they can be used as a means to bypass our security restrictions. VPN software is actively blocked, and persistent users can have their Wi-Fi access blocked.

2.6 Virtual Learning Environments

The College uses a Virtual Learning Environment platform called 'Firefly'. Wider use is made of a range of online applications such as Google WorkSpace for Education, Unifrog and other online applications. Activity on any VLE or online environment used by the College is subject to the conditions in this policy.

2.7 Personal devices

Members of the College community may wish to bring personally owned devices (laptops, tablets, mobile phones etc) into college. Please note such devices are not covered by the College's insurance. Where a student brings a personal device into the College for use in lessons, they must seek permission of the class teacher before using the device
(unless use of this device is deemed necessary by the SENCO). Security of such devices remains the responsibility of the individual. Please see section 3 of this document for additional detail.

2.8 Proper Use

The Internet is an important learning resource. Like any resource however it can be wasted or abused. When using the network and Internet facilities at Campbell College, students are expected to use their common sense and behave with normal standards of courtesy and should agree to the following terms:

- **Supervision:** Users will not use the system or any part of it without the permission of a member of staff. They should also understand also that they are not permitted to bring food or drink into the ICT Suites.
- **Vandalism:** Users will not purposely attempt to damage the hardware, software or data belonging to themselves or any other user on the system, either physically or through the purposeful introduction of a virus.
- **Inappropriate use:** Users will not waste college resources on unnecessary printouts, downloading or uploading large multimedia files.
- **Privacy and security:** Users will keep their passwords secret and not share them with anyone. Work saved under those usernames is the responsibility of the individual and part of their role as users is to keep it secure and backed up. Users will not attempt to access the system or any data on the system without authorisation; this includes access to another person's network files, email or portable storage media. A student may be held responsible for any actions carried out using their network-identity.

  If a student fails to keep his password secret another person may be able to delete or damage important files, such as coursework. The college cannot accept responsibility for damage where this is the case. The college will not accept responsibility for the loss of data.
- **Copyright:** Only software provided on the network may be run on the machines. College resources should not be used to illegally copy or download software for use in college or at home. Users understand that the Internet should not be used as a tool to aid plagiarism of coursework or any other assignment (see also Appendix 11 - Plagiarism and Use of Online Material Policy for Students)
- **Misuse:** Student users will use the system only for the tasks assigned to me by their teachers. Misuse includes but is not limited to, sending, or receiving messages containing pornographic or abusive content, inappropriate language, or illegal activities. The playing of on-line computer games is not an acceptable use of the ICT facilities in Campbell College.
- **Cloud storage / portable storage media:** The college preference for transfer of work between work and college is via Cloud Technology (Google Drive), all students have access to a Google Drive via their @ccblearning.org.uk login. Please use this account for storage and transfer of digital files that are needed outside of the college. Where digital files are stored on media such as USB pen drive, bit-locker encryption is needed before such devices can be used on the college network. Students should also understand that staff may inspect the material at any time. Students should not attempt to connect to the college network using electronic media without the permission of the college.

- **Content of websites and network folders:** Users accept that they must not include any text or images referring to any other Campbell College student, any staff members, or members of the Board of Governors of Campbell College in a website or any file saved on the college network without the prior permission of the person.

  The content of any folder stored on the college network, or any device connected to the network must never contain inappropriate content.

- **Safety:** Users understand that it is important not to disclose personal details across the Internet and that they should not arrange to meet in person with anyone they have "met" through the Internet.

  The Network Manager may make periodic snap checks on any electronic folder, PC, Laptop, or other electronic device.

Possible consequences for violating any portion of this agreement will be dealt with in line with the College's Positive Behaviour Policy.

2.9 The use of social media

Personal publishing tools include blogs, wikis, social networking sites (e.g. Facebook), bulletin boards, chat rooms and instant messaging programmes. These online forums are the most obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person.

The use of social media sites is barred from the college network, and students are not permitted to access social media sites while in college, in college uniform or when representing the College [exceptions are made for boarders as detailed in Appendix 5].
The College is aware that students do use such sites out of college. Because the College cannot control the use of the internet or media sites while under the supervision of parents/guardians, we ask that parents make their son fully aware how to block or report inappropriate messages or images on-line.

It is vital that parents supervise their son's activities on-line.

2.10 Published Content

No one may use the college name, badge, crest or motto or any identity associated with the College without express permission from the Headmaster or a Vice-Principal or the Marketing Department.

3. MOBILE PHONES AND PERSONAL DIGITAL DEVICES (mobile phones, smart watches etc)

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly.

Some issues surrounding the possession of these are:

- They can make students more vulnerable to cyber bullying,
- They can be used to access inappropriate internet material,
- They can be a distraction in the classroom,
- They are valuable items that could be stolen, damaged or lost,
- They have integrated cameras, which can lead to child protection, bullying and data protection issues.

The College takes certain measures to ensure that mobile phones (and other personal digital devices) are used responsibly in college:

- The College recommends that pupils do not bring mobile phones to school.
- Where pupils, with the permission of their parents, choose to bring a mobile phone to school, **they must be switched off and out of sight between the hours of 8.40 and 3.30.**
- The College will not tolerate cyberbullying against students or staff. Sending inappropriate, suggestive, or abusive messages is forbidden and anyone who is found to have sent a message of such content will be dealt with in line with the College's Addressing Bullying Policy and the Positive Behaviour Policy.
- Mobile phones can be confiscated by a member of staff, and the device may be searched by a Head of Year or a member of the Senior Leadership Team if there is reason to believe that there may be evidence of harmful or inappropriate use of the device.
- **Mobile devices must never be used to take sound, picture, or video clips of another person without their consent and the consent of a member of staff**.
- Sixth Form students may listen to music on a personal device in Study Hall only with the permission of the Study Supervisors.

Advice to students

Students are strongly advised:

- To ensure that there is nothing on their personal digital devices, chat rooms, websites, blogs or any other medium that supports the above-mentioned issues.
- To permanently delete any such material, photographs or language which may be viewed as crude, offensive or vulgar, which exists and may have been downloaded accidentally.
- To ensure that any unacceptable pictures of themselves or those taken of others; or material which brings discredit or disrepute upon, or which could damage the College's or a teacher's reputation in any way (including any comments about teachers or other students without their express prior knowledge and consent), should be urgently removed from the website or mobile phones or any other electronic apparatus.
- Their personal digital devices are never used without prior permission from a member of staff to take photographs or to record videos.

Advice to Parents

- It will not be possible to contact your son on his mobile device during the college day as he will not have access to his phone other than at break time and lunch time. Contact with your son can be made by telephoning Front of House.
- Ensure that if your son does carry a mobile phone that he is aware of the college policy regarding when he can use the phone and the restrictions on the use of the camera facility.
- Advise your son that he should never take or transmit an image of another without their prior consent.
- The college cannot police the use of mobile phones or other devices outside of college, so your son should be made aware of how to report any inappropriate use on-line or with the service provider.

APPENDIX 1

DIGITAL SAFETY AND ACCEPTABLE USE AGREEMENT FORM (STUDENTS)

As a student at Campbell College, I understand and agree to the following guidelines for using college ICT systems:

1. Personal Safety:
   - I acknowledge that my use of the systems, devices, and digital communications will be monitored by the college.
   - I will keep my username and password secure, not share them, and avoid storing them in easily accessible places.
   - I will exercise caution when communicating online, being mindful of "stranger danger."
   - I will not disclose or share personal information about myself or others, including names, addresses, email addresses, telephone numbers, age, gender, educational details, and financial details.
   - I will not arrange to meet unknown individuals online.
   - I will promptly report any unpleasant, inappropriate material, messages, or anything that makes me feel uncomfortable online.

2. Responsible Use:
   - College systems and devices are primarily for educational use; personal or recreational use requires permission.
   - I will not engage in large downloads or uploads that may hinder internet capacity for others.
   - Without permission from a staff member, I will not use college systems or devices for online gaming, internet shopping, file sharing, video broadcasting (e.g., YouTube), or online gambling.

3. Respectful Behaviour:
   - I will respect others' work and property, refraining from accessing, copying, removing, or altering files without permission.
   - I will communicate politely and responsibly, refraining from using strong, aggressive, or inappropriate language while appreciating differing opinions.
   - I will not post inappropriate or defamatory messages about Campbell College or its members.
   - I will not capture or distribute images of anyone without their permission, and I will not use mobile devices in college to take pictures or videos.

4. Internet Usage:
   - I will obtain permission when using others' original work in my own work.
   - I understand that downloading copyrighted material, including music and videos, is not allowed.
   - I will exercise caution when using the internet for research, ensuring the accuracy of information, and identifying deliberate attempts to mislead.
   - I will ensure any applications I use to enhance my work are used appropriately, ethically and are appropriately referenced.

5. Security and Integrity:
   - Personal digital devices may be used in college during breaks and lunch, following the rules outlined in this agreement.
   - I will not attempt to upload, download, or access illegal, inappropriate, or harmful materials, or bypass filtering/security systems.
   - I will promptly report any equipment or software damage or faults.
   - I will be wary of opening any email hyperlinks or attachments unless I am confident the senders address and reason for sending is legitimate.
   - I will not install or attempt to install or store programs on college devices or alter computer settings.
   - I will refrain from accessing or using social media sites during the college day or when representing the college.
   - Staff members have the right to confiscate personal equipment if there is a violation of this policy.

6. Personal Responsibility:

- The College reserves the right to take action for incidents of inappropriate behaviour outside of college if they involve my affiliation with the college community.
- I will not use the name, crest, or image of the College on any sites or posts without permission from a senior staff member.
- I will uphold the good reputation of the College and refrain from engaging in actions that bring disrepute.
- I will avoid posting insulting, degrading, or abusive messages about the College or any member on external platforms.
- Failure to comply with this policy may result in disciplinary action, including loss of network/internet access, detentions, suspensions, parental contact, and involvement of law enforcement for illegal activities.
- I will remain responsible for any personal digital devices I chose to bring into college; their physical safety and the security of their contents are my responsibility. I am aware that these devices are not covered by the College insurance policy.
- I am responsible for ensuring important work is saved appropriately on the college network and backed up using alternative means where necessary.
- I understand that where the use of a digital device which is my own property has been used inappropriately, it may be confiscated, and the contents examined.

By signing the agreement, I acknowledge that I have read, understood, and agree to abide by the Digital Safety and Acceptable Use Agreement. If you do not sign and return this, access will not be granted to school systems and devices.

DIGITAL SAFETY AND ICT ACCEPTABLE USE AGREEMENT

Please retain this policy document and return **this page only** to your Tutor. In instances where more than one student from a family attends Campbell College you are asked to complete a **separate sheet** for each student.

STUDENT AGREEMENT

I have read the Digital Safety Policy (incorporating the policy on the use of the internet, college network and electronic devices) and agree to follow these rules and guidelines. All of these guidelines apply while I am a student at Campbell College and all policies related to behavioural conduct also apply.

Student Name:_____

Year Group:_____ **House:**_____

Signature:_____ **Date:**_____

PARENT / GUARDIAN AGREEMENT

As the parent / guardian of the above student I give Campbell College permission to issue him with a network user account. I give permission for him to gain access to the Internet through the network facilities provided by Campbell College. I certify that he and I have read and understand the information contained in this agreement and agree to abide by all rules set out in this document. I understand that some material on the Internet is highly objectionable and accept responsibility for setting the standards he should follow when using the Internet.

Circle as appropriate: Yes / No

Signature: _____ **Date:**_____

(*I understand that I have the right to change my mind and withdraw consent and will contact the College if this is the case info@campbell.belfast.ni.sch.uk *)

APPENDIX 2

THE USE AND STORAGE OF IMAGES OF STUDENTS

Dear Parent / Guardian,

Re: The storage and use of visual images

You will have no doubt noticed how in Campbell we are delighted to celebrate the activities and achievements of our students in many ways and not least through photographs and video. On our website, in classrooms, on notice boards, in college publicity materials, in publications, on our Facebook page and via our Twitter feeds we display photographic records from a wide range of activities including class presentations, charity events, sporting activities or success of any nature. Taking, keeping and publishing photographs and video footage involves processing personal data under data protection laws. To enable us to comply with our obligations under the General Data Protection Regulation, we are required to obtain express consent to the use of a pupil's image. Therefore, after reading the following information, you will be asked to complete the **Storage and Use of Visual Images section of the Consent booklet**.

Background
In line with our Safeguarding and Child Protection Policy and Digital Safety Policy (available on our website www.campbellcollege.co.uk and from Front of House), we issue to all new students with Appendix 2, which deals with the storage and use of visual images. Through the policy we wish to take a pragmatic approach and allow the students and College to celebrate success and give credit and recognition for achievement. In recognition of our increase adoption of online media the College has introduced a Use of Social Media Policy (see Appendix 10) included within the Digital Safety Policy.

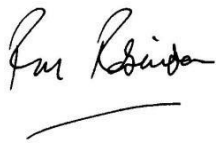
A college photograph is taken in Years 8, 11 and 13, and a copy of this is held on file electronically in accordance with the Data Protection Act. A copy is also available for you to purchase at that time. Other official photographs include a House photo and membership of any music groups or sports teams.

In addition to 'official' photographs, photographs and videos may be taken at various times throughout the year to recognise and enjoy the work of the students. The celebration of the success of our students is very natural and the students are delighted to see videos or photographs of themselves used in this way. The following are examples of the various platforms where such photographs or video may be used.

College Magazine:	The Campbellian
Print and Broadcast Media:	Radio, TV and Newspapers
Online:	College Website, College Facebook Page and College Twitter Feeds, College YouTube, College Vimeo and social media outlets of agreed College partners.
Other College Publicity:	College Prospectus, Open Days and similar publications.
Educational Materials:	Assessment and Teaching materials, for example, analysing sporting performance

I hope you find this useful regarding images taken by the college as well as any you may wish to take yourself. If you have any questions, please do contact Mr W Keown, Vice-Principal, or myself.

Yours sincerely



RM Robinson
Headmaster

From the Safeguarding and Child Protection Policy:

THE STORAGE AND USE OF IMAGES

The General Data Protection Regulation (GDPR) and Human Rights Legislation require that the College safely manages the use of photographs, videos and web cams in the college environment.

- All photographs held on file (both electronic and paper) of the students exist in accordance with the GDPR.
- Photographs and videos of the students taken during the year to promote the college for publicity use in the prospectus or in other printed material will be subject to consent by the parents. Images being used will portray the students appropriately attired.
- Digital video recordings may be made at various functions or of class activities. These can help encourage creativity, motivate, and enthuse students and improve communication, team-working skills and may be used for assessment purposes.
- Photographs of college staff will only be used with the consent of that staff member.
- Photographs taken for the purpose of journalism are exempt from the GDPR and on all occasions the students will be aware that their photograph may be used.
- Photographs or film footage by parents or guardians of their children at college events is permitted under an exemption in the GDPR.
- The use of camera phones or the internet to send offensive photographs to other students is not permitted and will be dealt with under the Discipline Code.
- Any incident of improper use of photographs/videos should be reported to a member of staff immediately.

ACTION BY THE COLLEGE

To protect student, we will:

- Seek their consent from parents for photographs/images to be taken or published,
- Ensure that photographs are appropriate,
- Encourage students to tell us if they are worried about any photographs that are taken of them,
- Reinforce the College policy that: Images / Sound / Video of a member of the College can only be taken with the consent of a member of staff AND with the consent of the person(s) involved.

THE STORAGE AND USE OF IMAGES OF STUDENTS

Please retain this policy document and return **this page only** to your Tutor. In instances where more than one student from a family attends Campbell College you are asked to complete a **separate sheet** for each student.

PARENTAL AGREEMENT

Student Name: _____

Year: _____ **House:** _____

I have read the policy and procedures contained within this document and the Digital Safety Policy and agree/disagree to the following:

1. I give consent for my child's image to be used in the College prospectus and other printed publicity material such as the college magazine in order to record and celebrate his/her success.

   YES / NO *Please circle your response*

2. I give consent for my child's image to be used on the College online resources, including College Ezines, Website, Facebook, Twitter, You-Tube, Vimeo or video recordings which may be used to record and celebrate occasions in the college year. This may also include recordings taken for assessment and teaching purposes.

   YES / NO *Please circle your response*

3. I give consent for my child's photograph to appear in the media including newspapers

   YES / NO *Please circle your response*

Parent/Guardian's signature:_____Date:_____

APPENDIX 3

DIGITAL SAFETY GUIDANCE FOR PARENTS

TOP TIPS FOR PARENTS:

Keeping children safe online is an important responsibility for parents in today's digital age. Here are some tips to help you protect your children while they are using the internet:

1. Open communication: Foster open and honest communication with your children about their online activities. Encourage them to share their experiences, concerns, and any issues they may encounter online.

2. Establish rules and boundaries: Set clear rules and boundaries regarding internet usage. Discuss appropriate websites, time limits, and the importance of responsible online behaviour. Ensure that your children understand and agree to these rules.

3. Educate about online dangers: Teach your children about the potential dangers of the internet, such as cyberbullying, inappropriate content, online predators, and scams. Help them recognize warning signs and understand the importance of privacy and personal information protection.

4. Use parental control software: Install parental control software or use built-in parental control features on devices and web browsers. These tools can help you filter content, set time limits, and monitor your children's online activities.

5. Keep devices in common areas: Encourage your children to use computers, tablets, and smartphones in common areas of the house, such as the living room or kitchen. This allows you to keep an eye on their online activities and prevents them from accessing inappropriate content in private.

6. Teach responsible social media usage: If your children are using social media platforms, educate them about responsible usage. Discuss the importance of privacy settings, the risks of sharing personal information, and the potential consequences of their online actions.

7. Monitor online activities: Regularly check your children's online activities without invading their privacy excessively. Maintain a healthy balance between trust and vigilance, ensuring that they are engaging in safe and appropriate online behaviour.

8. Encourage critical thinking: Teach your children to think critically about the information they come across online. Help them differentiate between reliable and unreliable sources, question the authenticity of content, and be sceptical of online offers or requests for personal information.

9. Foster empathy and digital citizenship: Emphasize the importance of empathy and respectful behaviour online. Teach your children about digital citizenship, including being kind, responsible, and ethical when interacting with others on the internet.

10. Lead by example: Be a positive role model for your children in your own online behaviour. Show them how to use technology responsibly, limit your own screen time, and prioritize real-world interactions.

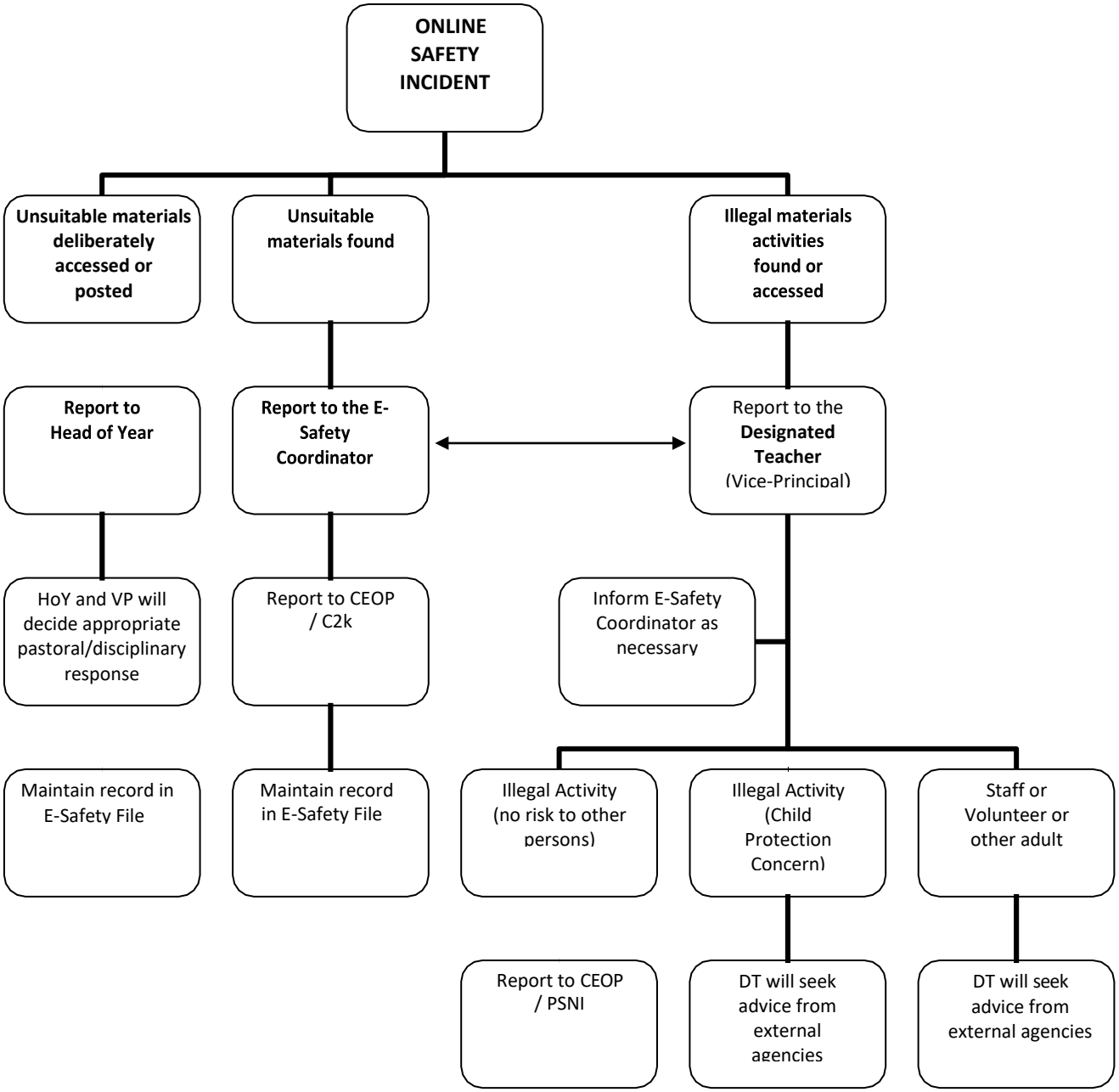
Remember that maintaining an ongoing dialogue and building a trusting relationship with your children is crucial for their online safety.

Useful advice for parents can be found on the Childnet site: www.childnet.com

Online reporting of inappropriate content can be done through the CEOP website **www.ceop.police.uk**

APPENDIX 4

GUIDANCE FOR STAFF ON DEALING WITH AN DIGITAL SAFETY INCIDENT



APPENDIX 5

CYBERBULLYING

(This section of guidance should also be read in conjunction with the COLLEGE ANTI-BULLYING POLICY)

DEFINITION

Cyberbullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. It can take different forms and guises including:

- **Email** – nasty or abusive emails which may include viruses or inappropriate content.
- **Instant Messaging (IM) and Chat Rooms** – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- **Social Networking Sites** – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- **Online Gaming** – abuse or harassment of someone using online multi-player gaming sites.
- **Mobile Phones** – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves, and these are subsequently transmitted to other people.
- **Abusing Personal Information** – may involve the posting of photos, personal information, fake comments, and blogs, or pretending to be someone online without that person's permission.

PREVENTATIVE MEASURES

- The College has an Anti-Bullying Policy and Procedures in place.
- Mobile phones are only to be used at break and lunch – never in class without permission.
- The camera function of any mobile device is banned in college.
- Social Networking sites are banned in college.

COLLEGE RESPONSE

For any incident involving Cyberbullying in college, the procedures described in the Anti-Bullying Policy will be followed.

STUDENT / PARENT RESPONSIBILITIES:

Parents and students should be aware how to prevent inappropriate or unwanted contact and how to report online. This should involve:

- **Setting appropriate privacy and filter settings.**
- **Blocking inappropriate contact or messages.**
- **Knowing how to report incidents online.**
- **Monitoring the use of the internet / social media sites at home.**
- **Abiding by the College rules on the use of the internet, mobile devices and social media.**

APPENDIX 6

DIGITAL SAFETY WITHIN THE BOARDING DEPARTMENT

All of the rules and procedures contained within this policy apply fully during the formal college day; however, there are a few additions and exceptions which apply within the boarding department after formal college hours.

GENERAL GUIDANCE

The following guidelines for acceptable use apply at all times.
All Boarding students are subject to the Campbell College Code of Conduct when using personal or college electronic devices:

Students are forbidden from:

- Downloading music/film which breaches copyright laws.
- Accessing gambling sites.
- Using unauthorised file-sharing sites.
- Using a proxy server with the intention of by-passing the College's 'safe' internet connection.

Students accept responsibility for the electronic equipment they bring to college and must ensure it is stored securely (and appropriately insured)
If the code of conduct is abused, sanctions may include confiscation of devices, or restrictions on the use of the internet during the evening and the weekend.

IMAGES OF STUDENTS

- No student may make a recording or take an image of another student without their prior consent must NEVER use a camera facility in private areas within boarding (e.g., bedrooms or bathrooms).

INTERNET ACCESS

For the Boarding Department, internet access on the College network is terminated at 23:00 hours each night. Some personal electronic devices may allow internet access or the creation of personal 'hotspots'. Students may only connect to their own hotspot, which must be password protected. They must not allow others to connect to their hotspot and will be responsible for the safety of their personal password. Students remain responsible for their electronic safety when accessing the internet via their own mobile device and must abide by the terms and conditions contained within the Digital Safety policy. See also the college policy on the use of VPN's on page 7 of this document.

SOCIAL MEDIA ACCESS

All students are forbidden from accessing social media sites during the college day; however, for Boarders they can be a key form of communication with family and friends. Social networking sites may be accessed through personal electronic devices but that is conditional on their safe and responsible use.

Students must:

- Ensure their privacy settings are set correctly and not to 'open access'
- Only accept friend requests from friends!
- Not engage in conversations on-line with people they do not know
- NEVER post inappropriate pictures or contact details about themselves
- NEVER post an inappropriate or defamatory message about another person
- Know how to report or block inappropriate messages on-line
- Report any inappropriate activity on-line to a member of staff.

APPENDIX 7

ELECTRONIC DEVICES: SEARCHING AND DELETION

The Positive Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of banned items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices. Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices / data where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the college rules.

- Searching with consent - Authorised staff may search with the student's consent for any item.
- Searching without consent - Authorised staff may only search without the student's consent for anything which is either 'prohibited' or appears in the college rules as an item which is banned.

CARRYING OUT A SEARCH

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places eg an occupied classroom, which might be considered as exploiting the student / student being searched.
Ideally a second member of staff should be present.

ELECTRONIC DEVICES

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident.

If inappropriate material is found on the device <u>it is up to a Vice-Principal</u> (Designated Teacher) to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of college discipline) or whether the material is of such seriousness that it requires the involvement of the police.
If in doubt the device may be confiscated, and an external agency (such as a designated Board Officer, Social Services or Police) may be contacted for advice.
Examples of illegal activity would include:

- **child sexual abuse images (including images of one child held by another child)**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

DELETION OF DATA

An item which may cause hurt or offence to others (<u>which does NOT constitute an illegal activity</u>) may be deleted to avoid it being transmitted to others.

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a <u>good reason</u> to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the college rules).

If an item or file is to be deleted from an electronic device, two members of staff should be present and a record should be kept containing the time, date and who was present along with a brief description of the offending item/data. The record will be held in the Digital Safety Incident File.

If there is any doubt, a Vice-Principal (or Designated Teacher) should be contacted.

APPENDIX 8

CONTACTS AND RESOURCES

Child Exploitation and Online Protection (CEOP) www.ceop.police.uk

CEOP works with child protection partners across the UK and overseas to identify the main threats to children and coordinates activity against these threats to bring offenders to account.

CEOP also offers an on-line reporting mechanism to report inappropriate on-line activity.

Think U Know?

www.thinkuknow.co.uk

ThinkUKnow is a resource developed by CEOP to educate young people about on-line dangers. Resources are available for young people, adults and teachers. It includes the latest information on the sites young people visit, mobiles and new technology. There is also the facility to report content if they feel uncomfortable or worried about someone they are chatting to online.

Childline

www.childline.org.uk

Provides on-line advice on all child protection issues, including Digital Safety.

Childnet

www.childnet.com

Provides on-line resources and advice on on-line activity to young people, parents and young people.

APPENDIX 9

DIGITAL SAFETY GUIDANCE FOR STAFF

'Staff' applies to all employees of Campbell College and all adults acting in a supervisory capacity at the College.

This Policy is intended to:

- ensure that staff are responsible users and stay safe while using the internet and other communications technologies;
- ensure that college ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- ensure that staff are protected from potential risk in their use of ICT in their everyday work

Personal Use

Campbell College's ICT systems are intended for educational use and to help with the smooth running of the College. Limited and 'reasonable' personal use of the Internet and other ICT facilities is permitted within the boundaries of reasonable use detailed below.
Reasonable Use:

- Is lawful and ethical;
- Is in accordance with this policy;
- Takes place during authorised breaks, non-contact periods or outside of working hours;
- Does not adversely affect your productivity, or interfere with teaching & learning activity;
- Does not make unreasonable use of College resources.

Acceptable Use

All staff and volunteers are expected to be professional in any communications and actions when using College ICT systems. Although not exhaustive the following is a list of "do's and don'ts".

- They will not access, copy, remove or otherwise alter any other user's files, without their permission.
- They will communicate with others in a professional manner
- Publishing information about the College, including its staff, students and parents, should only be carried out with the prior approval of the Headmaster or a Vice-Principal or the Marketing Department
- **Staff should not set up a web-site or internet group without the prior permission from the Headmaster or a Vice-Principal. They will, in turn discuss the proposal with the Marketing Department.**
- They will not communicate with current students via social networking sites.
- They will not engage in any on-line activity that may compromise their professional integrity and suitability to work at Campbell College.
- Staff and volunteers must not defame College staff, parents, students or misrepresent or negatively publicise Campbell College on any public information system.
- They must not disclose confidential information about the College or post content that could harm the image of the College.
- They must not bring the College into disrepute through any use of ICT.

Use of own Cameras/Personal Mobile Devices for college use

A college camera is available for staff to use; however, there may be times when staff take an image of a student on their own device for official college use. All such images should then be transferred onto college devices as soon as possible and any images deleted off a personal device. Ideally, this should be done within 24 hours or as soon after the event as possible. Images should not be retained for longer than is necessary.

Personal Use of Social Media

When using personal channels of Social Media individuals should never identify themselves as members of the Campbell College community unless specifically linked to an approved role or activity that has been sanctioned by the College. This is to safeguard the privacy of all members of staff, students, parents and the wider Campbell Community.

Staff should set their privacy settings so that personal information such as posts, images or contact details cannot be viewed or accessed by unauthorized users.

Students should not have contact through any personal social medium with any member of staff other than via mediums approved by the Leadership Team, unless the staff concerned are direct family members.

Photographs, videos and any images that contain students, members of staff, their families, feature images of the college premises, feature any of the College emblems or reference the College in anyway should only be used in accordance with this policy and with approval of the Marketing Department.

College email addresses must not be used to set up personal social media accounts.

Campbell College is responsible for providing safe and secure access to technologies:

- Usernames and passwords must not be disclosed to anyone else, nor must anyone try to use any other person's username and password.
- Use of personal external devices (for example PDAs, laptops, mobile phones, USB devices etc) in College, whether issued by the College or otherwise, is subject to the rules set out in this policy. If such devices are used to access the College's ICT systems, they must be protected by up-to-date anti-virus software and be free from viruses.
- Attachments to emails should not be opened, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Data should be regularly backed up.
- Staff must not attempt to upload, download, access or forward any materials which are illegal or inappropriate (for example, child sexual abuse images, racist material, pornography) or may cause harm or offence to others. This includes violent material or that which glorifies violence; criminal, terrorist, or glorified criminal activity; unsuitable sexual content; blasphemous material or that which mocks any religious and moral beliefs or values.
- Staff have a duty to report immediately any illegal, inappropriate, or harmful material or incident, of which they become aware in line with this policy.
- They must not try to use any programmes or software that might enable the bypassing of the filtering and security systems in place to prevent access to such materials or restricted areas of the ICT systems.
- Staff must only transport, hold, disclose or share personal information about themselves, or others, as outlined in the College Data Protection Policy. The Data Protection Policy requires that any staff or student data to which staff have access, will be kept private and confidential, except when it is deemed necessary or required by law or by college policy to disclose such information to an appropriate authority.
- Any damage or faults involving equipment or software; however, this may have happened, must be reported to the Network Manager immediately.
- Where work is protected by copyright, it must not be downloaded or distributed.

Safeguarding (Child Protection) Policy

- Staff should be aware of the guidance and procedures detailed with the Safeguarding Policy

APPENDIX 10

POLICY ON THE USE OF SOCIAL MEDIA ASSOCIATED WITH CAMPBELL COLLEGE

This Policy applies to all staff, students and the wider Campbell College community who choose to engage with the College on any of our online platforms including the College Website, our Virtual Learning Environment (FireFly) and social media associated with the College such as Facebook, Twitter, You-Tube etc.

Protection of Campbell College Identity

The Campbell College Crest and associated emblems are, under no circumstances, to be used or published on any personal online space without prior written consent from the College. These are registered trademarks with Royal Charter status and are the intellectual property of Campbell College only.

Conduct on Electronic Media

All communication on media must be in line with the standards detailed in the

- Digital Safety Policy and ICT Acceptable Use Agreement (for Students)
- Digital Safety Guidance for Staff

Official Campbell College Channels

Campbell College Marketing Department oversees and manages the content of the Website, Facebook, Twitter and YouTube channels.
Individuals are encouraged to interact with these official online channels but to do so in a responsible and respectful manner. All channels are monitored and should any inappropriate behaviour on any medium occur disciplinary action may be taken and the individual may be blocked and reported to the relevant service provider.

Campbell College used other specified media for communication with and between staff and students and due care and consideration must also be applied by all users in this context.

Monitoring

All official online platforms are reviewed by the Senior Leadership Team and the Marketing Department and any breach of this policy will be treated with an appropriate response.

If used wisely, the online world will help us to share what makes Campbell College unique.

APPENDIX 11

PLAGIARISM AND USE OF ONLINE MATERIAL POLICY (for students)

This policy aims to educate students about the importance of academic integrity, specifically regarding plagiarism and the appropriate use of online material, including AI-generated content. It establishes guidelines for responsible and ethical conduct when using online resources to complete assignments, projects, or any other academic work.

1. Definition of Plagiarism:

Plagiarism is the act of presenting someone else's work, ideas, or words as one's own without giving proper credit or citation, (this is an infringement of the Copyright, Designs and Patents Act). This includes, but is not limited to, copying, and pasting text from websites, using someone else's ideas or thoughts without attribution, and submitting another student's work as your own.

2. Responsible Use of Online Material:

- **Research and Citation:** When conducting research online, students must critically evaluate the information and ensure the accuracy and reliability of the sources. Proper citation and referencing should be used to acknowledge the original authors or creators of the content.
- **Paraphrasing and Summarizing:** If using information from online sources, students should practice paraphrasing or summarizing the content in their own words, giving credit to the original source through appropriate citations.
- **Creative Commons and Public Domain:** Students should familiarize themselves with the concepts of Creative Commons licenses and public domain materials. They should adhere to the specific usage guidelines outlined by the respective licenses when incorporating such content into their academic work.

3. Use of AI-Generated Content:

- **Transparency:** If students utilize AI-generated content or tools to assist in their academic work, they must clearly indicate the use of AI technology and identify the sources or tools employed.
- **Evaluation and Originality:** While AI-generated content may provide assistance, students must ensure that their final work reflects their own understanding and originality. Merely relying on AI-generated content without proper comprehension and personal input is not acceptable.
- **Citation and Attribution:** If AI-generated content is used directly in academic work, students must provide appropriate citations or attributions to the AI system or tool utilized, following the guidelines provided by their educational institution. (See also Appendix 12)

4. Consequences of Plagiarism:

Plagiarism is a serious academic offense that undermines the learning process and violates ethical standards of the College.

The consequences for plagiarism may include, but are not limited to, the following:

- Reduced or failing grades for the assignment or project.
- Academic probation or disciplinary action as per the college's policies.
- Damage to the student's reputation and future academic opportunities.

5. Education and Awareness:

- Colleges should provide students with educational resources, workshops, or training sessions to enhance their understanding of plagiarism and responsible use of online material, including AI-generated content.
- Teachers and educators should incorporate discussions on academic integrity and plagiarism prevention into their curricula, reinforcing the importance of originality, critical thinking, and proper citation.

6. Support and Guidance:

Colleges should ensure that students have access to guidance and support from teachers, librarians, or other relevant personnel who can assist them in understanding and adhering to the policies outlined in this document. Students should feel comfortable seeking clarification or advice when it comes to using online material and avoiding plagiarism.

7. Regular Policy Review:

This policy should be reviewed periodically to ensure its relevance and effectiveness in addressing emerging issues related to plagiarism, online material, and the use of AI in academic settings. Any necessary updates or modifications should be made to align with best practices and the evolving landscape of technology and academic integrity.

Conclusion:

By adhering to this policy, students will foster a culture of academic integrity, uphold ethical standards, and develop critical thinking skills necessary for their educational journey. It is essential for students to understand the importance of originality, proper citation, and responsible use of online material, including AI-generated content, to succeed.

APPENDIX 12

USING GENERATIVE AI - ARTIFICIAL INTELLIGENCE (for students)

This policy is informed is informed by JCQs paper, AI Use in Assessments and the government's white paper on a pro-innovation approach to AI regulation.

What is generative AI?
Technology such as ChatGPT or Google Bard are examples of generative AI. The are technologies that can be used to create new content based on large volumes of data.

Examples of tasks generative AI can complete include:-

- Answering questions and completing written tasks in a human like way.
- Creating audio, code, image, video, or text files in response to a description provided.

What to do if you use generative AI to help you complete a task?
It remains essential that students are clear about the importance of referencing the sources they have used when producing work for an assessment, and that they know how to do this. Appropriate referencing is a means of demonstrating academic integrity and is key to maintaining the integrity of assessments. If a student uses an AI tool which provides details of the sources it has used in generating content, these sources must be verified by the student and referenced in their work in the normal way. Where an AI tool does not provide such details, students should ensure that they independently verify the AI-generated content – and then reference the sources they have used.

What is appropriate use of generative AI?

- Supporting research into a topic to help initial understanding or insight.
- As a conversational or debating partner to help you develop ideas
- Help drafting ideas of suggesting structures for a written task.
- Generating image or other multimedia content to support a presentation or report, but not where the task itself requires you to create your own original multimedia illustration.
- Generating questions from an article or text to help you assess your understanding of the content.
- Help you improve your grammar or writing structure, especially useful if English is a second language.
- Debugging code, but the code uploaded for evaluation must be original in the first instance and must be clearly commented to show your own understanding of the processing carried out.

What to be aware of if you do use generative AI

- The content generated can sometimes be inaccurate, out of date or inappropriate.
- Content generated by AI can be subject to bias.
- It stores data you provide it with and will learn from that data. Personal or other data shared on AI (as with social media), has the potential to become publicly available.
- AI does not respect copyright laws. Original data, images, and other content you upload and which you own the intellectual property rights to can be become available for reuse by others without your permission.
- References and citations provided by AI can be fictitious; evaluate content linked to references provided.
- Misuse of AI will be considered academic misconduct.