CAMPBELL
COLLEGE

Est 1894

E-SAFETY AND ICT ACCEPTABLE USE POLICY

Revised:	**June 2017**
Next Revision:	**June 2019**

DESIGNATED STAFF FOR E-SAFETY

Electronic Safety Coordinator	**Mrs M Debbadi (Head of ICT)**
Network Manager / IT Technical Support	**Mr S Liggett / Mr M Lyttle**
Designated Teacher for Child Protection	**Mr C Oswald (Vice-Principal)**

1. ELECTRONIC SAFETY

Electronic Safety (E-Safety) covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technologies. The rapidly changing nature of the internet means that e-Safety is an ever growing and changing area of interest and concern.

This policy applies to all members of the school 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 school.

1.1 LINKS TO OTHER POLICIES

This policy should be read in conjunction with the other policies of the College in particular those concerning Safeguarding and Child Protection, Positive Behaviour, Anti-Bullying and Pastoral Care.

1.2 APPENDICES

Appendix 1	**E-Safety and Acceptable Use Agreement (for Students)**
Appendix 2	**Use of images and Photographs of Students**
Appendix 3	E-SAFETY CHECKLIST FOR PARENTS
Appendix 4	**Guidance on dealing with an E-Safety Incident**
Appendix 5	**Cyberbullying**
Appendix 6	**E-Safety within the Boarding Department**
Appendix 7	**Electronic Devices: Searching and Deletion**
Appendix 8	CONTACTS AND USEFUL RESOURCES
Appendix 9	**E-Safety and Acceptable Use for Staff**
Appendix 10	**Use of Social Media Policy**

1.3 ROLES AND RESPONSIBILITIES

E-Safety Coordinator

- Takes day-to-day responsibility for e-Safety issues and has a leading role in establishing and reviewing the College's e-Safety policies, documents and procedures
- Ensures all staff are aware of the procedures that need to be followed in the event of an e-Safety incident, and provides training and advice to staff
- Liaises with the College's technical staff
- Receives reports of e-Safety incidents and keeps a log of incidents to inform future e-Safety developments
- Develops curriculum resources for the promotion of e-Safety across the curriculum
- 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 e-Safety requirements and guidance issued by the Department of Education, both on C2k and legacy equipment
- Ensures that users may only access the networks and devices through properly enforced passwords, which are changed regularly
- Regularly monitors the use of the network / internet / VLE / remote access and email in order that any misuse is reported to the e-Safety Coordinator
- Ensures that any software / systems are implemented/uploaded in line with school policy

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.)

Teaching and Support Staff

- Have an up to date awareness of e-Safety matters and the current e-safety policy and practices
- Have read and understood this policy
- Report any suspected misuse or problem to the relevant Head of Year/Tutor
- Keep any form of communications with students / parents / guardians to a professional level (and carried out using official school systems)
- Ensure they and students avoid plagiarism and uphold copyright regulations
- In lessons which involve the use of electronic media / internet, to check the suitability of all material before the lesson.
- To ensure students know to report any unsuitable material that is found in internet searches

Students

- Students are responsible for using the College digital technology systems in accordance with this policy
- Should avoid plagiarism and uphold copyright regulations
- 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 mobile devices (such as mobile phones and cameras)
- Should understand the College's stance on Cyber-bullying
- Should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the College's policy covers their actions out of school, if directly related to their membership of the school (though the College cannot police the internet when the students are in the care of their parents/guardians)

Parents / Guardians **(see Appendix 3)**

Parents play a **crucial** role in ensuring that their son understands the need to use the internet / mobile devices in an appropriate way. We ask that parents support the College in promoting good e-Safety at home and ensure that they and their son follow guidelines on the appropriate use of:

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

1.4 PROFESSIONAL DEVELOPMENT FOR STAFF

The e-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 e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety needs of all staff will be carried out regularly
- All new staff will receive e-Safety training as part of their induction programme, ensuring they fully understand the school e-Safety policy and acceptable use arrangements
- The e-Safety Coordinator will receive regular updates through attendance at external training events when offered
- This e-Safety Policy will be presented to and discussed by staff in team meetings / Staff Development Days
- The e-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 access by the headmaster (or designated deputy)

1.5 E-SAFETY AND INTERNET ACCEPTABLE USE AGREEMENT FORM

We ask students and parents to read the contents of this policy, to discuss the e-Safety guidance given in **Appendix 1** and to sign and return the agreement section.

1.6 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 (eg 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 school.

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

1.7 E-SAFETY EDUCATION

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

- A planned e-Safety curriculum is provided as part of ICT and LLW lessons
- Key safety messages are reinforced as part of a planned programme of tutor periods, year Assemblies and School 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 C2k system is monitored and security reports can be accessed.

We provide information and awareness to parents through:

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

1.8 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 school must remain under their personal care and they must ensure it is stored securely and properly insured.

1.9 COMMUNICATION OF THIS POLICY

This policy will be made available to all staff on the C2k network and will be available to students and parents either on the College Website, or by requesting a hard copy.

1.10 PROCESS OF REVIEW

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

2. INTERNET AND NETWORK ACCEPTABLE USE

We are very pleased to be able to offer a wide range of information technologies to students and staff at Campbell College. Our main goals in providing these resources are to promote educational excellence through research, communication, increased independent learning, exposure to new and developing industry standard applications and interactive learning environments. It is to be remembered however that access to the ICT facilities provided by Campbell College is a privilege that should not be abused and as such is subject to a variety of terms and conditions. In order to limit possible misuse of the ICT facilities at Campbell College, we require students and parents to read, understand and agree the following.

2.1 Passwords

Each student will be assigned a password (or passwords) for use with the Campbell College Network. The password selected should be something the student will easily remember but it should not be obvious to other students.
Students 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 staff so a new password can be issued.

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

Students will be required to update their C2K password at least once a term. Responsibility to do this lies with the individual student and failure to do so will result in an automatic lockout from the C2K system when the password automatically expires. Reminders will be issued and facilities provided to enable students to update passwords regularly.

2.2 WiFi Access (through C2k / College WiFi)

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.

2.3 Internet Access via mobile devices (e.g. 3G and 4G Datacards) 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 Virtual Learning Environments

The College uses a Virtual Learning Environment platform called ‘Firefly’. Activity on any VLE used by the College is subject to the conditions in this policy.

2.5 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:** I will not use the system or any part of it without the permission of a member of staff. I understand also that I am not permitted to bring food or drink into the ICT Suites.
- **Vandalism:** I will not purposely attempt to damage the hardware, software or data belonging to myself or any other user on the system, either physically or through the purposeful introduction of a virus.
- **Inappropriate use:** I will not waste school resources on unnecessary printouts, downloading or uploading large multimedia files.
- **Privacy:** I will keep my own passwords (legacy and C2K) secret and not share them with anyone. The work saved under those usernames is my responsibility and I should keep it secure and backed up. I 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, then another person may be able to delete or damage important files, such as coursework. The school cannot accept responsibility for damage resulting from a student's failure to keep their password secure.
- **Security:** It is my responsibility to ensure that work saved on either of the Campbell College networks is held securely and backed-up so that corrupt files, or lost data, can easily be recovered. **The school will not be responsible for the loss of files**.
- **Copyright:** Only software which has been provided on the network may be run on the machines and school resources should not be used to illegally copy or download software for use in school or at home. I also understand that the Internet should not be used as a tool to aid plagiarism of coursework or any other assignment.
- **Misuse:** I will use the system only for the tasks assigned to me by my teachers. Misuse includes but is not limited to, sending or receiving messages containing pornographic or abusive content, inappropriate language or illegal activities. I also understand that the playing of on-line computer games is not an acceptable use of the ICT facilities in Campbell College. I understand that all online activity is automatically tracked and recorded by an external organisation.
- **Electronic media:** I will only make use of CD-ROMs, pen drives etc with the approval of my subject teacher and on the understanding that any member of staff may inspect the material at any time. I should not attempt to connect to the school network using electronic media without the permission of the school.
- **Content of websites and network folders:** I understand that I 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 school network without the prior permission of the person.
- **The content of any folder stored on the school network or any device connected to the network must never contain inappropriate content.**
- **Safety:** I understand that it is important not to disclose personal details across the Internet and that I should not arrange to meet in person with anyone I have "met" through the Internet.

Students should understand that all on-line activity is tracked and recorded by an external organisation. 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.

2.6 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 school network, and students are not permitted to access social media sites while in school, in school uniform or when representing the College [exceptions are made for boarders as detailed in Appendix 6].

However, the school is aware that students do use such sites out of school. Because the school 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.

The College will always be available to advise parents should an incident occur outside of school control, but incidents beyond the school day are primarily the responsibility of parents.

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

2.7 Published Content

No one may use the school 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 DEVICES

While mobile phones and personal communication devices are commonplace in today's society, 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 a 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 devices) are used responsibly in school:

- Mobile phones may only be used at break and lunch and never during class
- 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 Anti-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 nothing which they have on mobile phones, chat rooms, websites, blogs or any other medium could lead to this situation arising,
- to wipe off 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 the school or which could damage the School'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 mobile phones are never used without prior permission from a member of staff to take photographs.

Advice to Parents

- You should not contact your son during class when he will be unable to take the message. 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 school 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 school cannot police the use of mobile phones or other devices outside of school, so your son should be made aware of how to report any inappropriate use on-line or with the service provider.

APPENDIX 1

<u>E-SAFETY AND ACCEPTABLE USE AGREEMENT FORM (STUDENTS)</u>

As a student at Campbell College, I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it and use it.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will not arrange to meet people on-line who I do not know
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use, unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for online gaming, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- I will never use the school systems for online gambling.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not post any form of inappropriate or defamatory message about Campbell College, or any member of Campbell College
- **<u>I will not take or distribute images of anyone without their permission, and I will not use any mobile device in school to take pictures or videos</u>**

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / iPods etc) in school at break and lunch and if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not access or use Social Media sites during the school day or when representing the school
- I understand that staff have the right to confiscate any items of personal equipment when I have, or it is suspected that I have broken the guidance and rules within this policy,

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they specifically involve my membership of the school community.
- I will not use the name, crest or image of the College, on any sites or posts unless I have permission from a senior member of staff of the College.
- I will not bring the good name of the College into disrepute.
- **If I am using ICT outside school, I will not post insulting, degrading or abusive messages about the College or any another member of the College.**
- I understand that if I fail to comply with this Policy, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in this document. If you do not sign and return this agreement, access will not be granted to school systems and devices.

E-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 Electronic 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: ________________ **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: ______________________

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 school 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. For your child to be involved we require your consent and I would ask you to read the following information and return the completed Consent Form. (Please retain the other pages for your records).

Background

In line with our Safeguarding and Child Protection Policy and E-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 School has introduced a Social Media Policy included within the E-Safety Policy.

A school 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.

School Magazine:	The Campbellian
School Ezine:	Campbell Life/Old Campbellian Ezine
Print and Broadcast Media:	Radio, TV and Newspapers
Online:	School Website, School Facebook Page and School Twitter Feeds, School You –Tube, School Vimeo and social media outlets of agreed School partners.
Other School Publicity Materials:	School Prospectus, Open Days etc

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

Yours sincerely

RM Robinson
Headmaster

From the Safeguarding and Child Protection Policy:

THE STORAGE AND USE OF IMAGES

The Data Protection Act (DPA) and Human Rights Legislation require that the College safely manages the use of photographs, videos and web cams in the school environment.

- All photographs held on file (both electronic and paper) of the students exist in accordance with the DPA.

- Photographs and videos of the students taken during the year to promote the school 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 school staff will only be used with the consent of that staff member.

- Photographs taken for the purpose of journalism are exempt from the DPA 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 school events is permitted under an exemption in the DPA.

- 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 Electronic 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 school 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 School Ezines, Website, Facebook, Twitter, You-Tube, Vimeo or video recordings which may be used to record and celebrate occasions in the school 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

E-SAFETY GUIDANCE FOR PARENTS

The internet is an exciting and diverse place full of opportunities and containing massive quantities of resources. However, for many parents and guardians, who can sometimes have less experience of the online world, it can be a concerning place.
Some of the risks include:

- Safety when communicating online: do you *really* know who you are communicating with?
- The safe, respectful (and lawful) use of Social Media sites: what you post online stays online!
- Safety when accessing sites that may have inappropriate content: some content is illegal.

TOP TIPS FOR PARENTS:

1. Ensure you have the correct 'parental control' settings including setting your favourite search engine (such as Google, Bing etc) to 'safe searches'.

This will make sure that a search returns content suitable for all ages. On most home screens for a search engine, there is an option under 'settings'. This should filter out most inappropriate content,

2. Encourage your family to use technology in a public part of the house

Keep the family computer in a central location (not in bedrooms), where it's easier to monitor what your children are doing. If your child has their own computer, encourage them to use it at home in public space.
This applies not just to PCs but also to laptops, iPads, E-Readers and games consoles.
Electronic devices should not be used late at night as this affects sleep patterns and ultimately their learning.

3. Encourage your child always to tell you if they receive suspicious or unwanted messages.

Encourage your child not to open emails from unfamiliar email addresses and to avoid opening suspicious attachments. As far as possible you should encourage your child to use an email address that you know and trust. Granted, as children get older they wish to be more private about their communications with others, which is understandable! It is all about being responsible.

4. Tell children NEVER to give out their personal details whilst online

If they want to subscribe to any online services or websites make up a family email address to receive the mail.

5. Ensure your son knows how to report or block inappropriate or unwanted messages.

Most search engines and social media sites have a facility to report inappropriate content, but do they know how to do that? Guidance is given by each of these media and by service providers.

6. Ensure your son knows the rules when using Social Media sites (such as Facebook, Instagram, Bebo, MSN etc.)

- To set up an account on the likes of Facebook and Instagram you must be over 13.
- He should have the correct privacy settings so his profile is not public and only accept friend requests from true friends.
- He must never post anything insulting, nasty or upsetting messages about another individual or the College
- You should know how to block and/or report unwanted posts.
- DO NOT ACCEPT FRIEND REQUESTS FROM ANYONE EXCEPT TRUSTED FRIENDS!

7. Ensure your son knows that he should <u>never</u> send anyone inappropriate pictures of himself, or send on inappropriate pictures of anyone else.

Sending sexually explicit pictures electronically (of other people or themselves) is illegal and can lead to PSNI involvement. The term '*sexting*' is the sending of sexually explicit pictures via text (but equally applies to sending pictures via any other form of e-media).

It is important that the message is reinforced:

"Never send something online that you would not want all your family and friends to see"

"If anyone asks you to send them a picture of yourself – DON'T"

"If you receive an image you know to be wrong DO NOT SEND IT ON – Report it"

ANYTHING you post online can be made widely available.

Child protection concerns are discussed in the Safeguarding Policy.

8. KNOW YOUR SON'S PASSWORDS / PASS CODES

Make your son aware that you can access any device at any stage – and do check that. Young people are vulnerable and sometimes do not think about their actions. If they know you can (and do) look at their electronic devices they are more inclined to make better decisions.

<u>GUIDANCE DOCUMENTS FOR PARENTS</u>

We have published a number of documents for parents on our website (go to About – Policies – Guidance). Copies may also be made available by contacting the College. You should also see APPENDIX 8.

Keeping your child safe online

A checklist for parents (produced by CEOP).

keeping up with children on the internet...

...an internet safety guide for parents, carers and teachers

Internet Safety

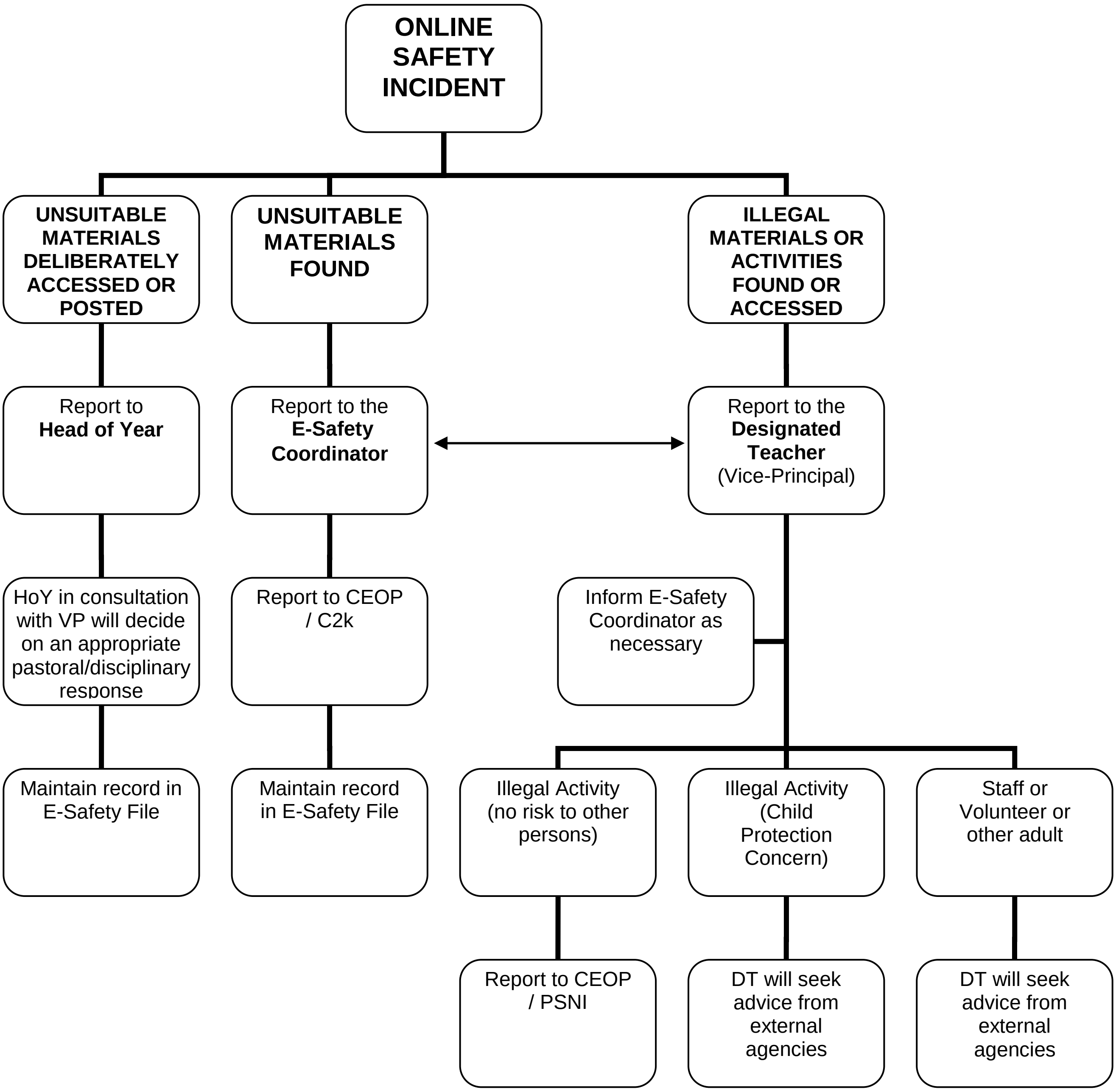
Keeping up with children (produced by Childline).

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 E-SAFETY INCIDENT



ONLINE SAFETY INCIDENT
UNSUITABLE MATERIALS DELIBERATELY ACCESSED OR POSTED
UNSUITABLE MATERIALS FOUND
ILLEGAL MATERIALS OR ACTIVITIES FOUND OR ACCESSED
Report to Head of Year
Report to the E-Safety Coordinator
Report to the Designated Teacher (Vice-Principal)
HoY in consultation with VP will decide on an appropriate pastoral/disciplinary response
Report to CEOP / C2k
Inform E-Safety Coordinator as necessary
Maintain record in E-Safety File
Maintain record in E-Safety File
Illegal Activity (no risk to other persons)
Illegal Activity (Child Protection Concern)
Staff or Volunteer or other adult
Report to CEOP / PSNI
DT will seek advice from external agencies
DT will seek advice from external agencies

APPENDIX 5

CYBERBULLYING

(REFERENCE 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 may only be used with permission from staff
- Social Networking sites are banned in school (the exception being in the evening for Boarders)

COLLEGE RESPONSE

For any incident involving Cyberbullying in school, 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

E-SAFETY WITHIN THE BOARDING DEPARTMENT

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

SOCIAL MEDIA ACCESS

All students are forbidden from accessing social media sites during the school 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

<u>ELECTRONIC DEVICES: SEARCHING AND DELETION</u>

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 school 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 school 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) or the <u>Headmaster</u> to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school 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 school 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 E-Safety Incident File.

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

APPENDIX 8

CONTACTS AND RESOURCES

UK Safer Internet Centre
www.saferinternet.org.uk

UK Safer Internet Centre, where you can find e-safety tips, advice and resources to help children and young people stay safe online

VODAPHONE DIGITAL PARENTING MAGAZINE

Vodaphone produce a 'digital parenting' online magazine giving useful tops and the latest information on keeping your child safe online.

http://www.vodafone.com/content/digital-parenting.html

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 e-safety.

Childnet
www.childnet.com

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

APPENDIX 9

E-SAFETY GUIDANCE FOR STAFF

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

This Acceptable Use Policy is intended to:

- ensure that staff are responsible users and stay safe while using the internet and other communications technologies;
- ensure that school 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 School. Limited and ‘reasonable’ personal use of the Internet and other ICT facilities is permitted within the boundaries of reasonable use detailed below. However, personal emails should not be sent on any of the College’s accounts. ICT usage and email can be recovered and viewed.

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 School resources.

Acceptable Use

All staff and volunteers are expected to be professional in any communications and actions when using School 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 School, 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 School or post content that could harm the image of the School.
- They must not bring the School into disrepute through any use of ICT.

Use of own Cameras/Personal Mobile Devices for school use

A school 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 school use. All such images should then be transferred onto school 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 School. 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 school premises, feature any of the School emblems or reference the School in anyway should only be used in accordance with this policy and with approval of the Marketing Department.

School 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 School, whether issued by the School or otherwise, is subject to the rules set out in this policy. If such devices are used to access the School’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 (for example, child sexual abuse images, racist material, pornography) or inappropriate 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 School 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 school 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

- **Scope**

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 School. 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

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

We are delighted to have the support of our students, parents and our staff on social media and recognise the importance of this medium as a way of connecting our Campbell Community. However, social media is not the appropriate forum to voice specific complaints. We would rather deal with issues in person to ensure they are dealt with effectively, professionally and in a respectful manner to all parties involved.

Hence, any concerns and complaints regarding the College should be raised in accordance with our policy: directly to the College and by the person raising the concern and not via social media platforms.

- **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 behavior 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.