INTERNET & SAFETY POLICY

PRIMARY PERSON RESPONSIBLE FOR IMPLEMENTATION AND MONITORING OF THIS POLICY

JAMES EYTLE, BEVERLEY MELLON (PRINCIPALS)

LAST REVIEW DATE

Jan 2018

NEXT REVIEW

Jan 2019

Internet and e-Safety Policy

1. Introduction

We believe that the Internet is a vital tool for modern education; it is a part of everyday life for academic work and social interaction in schools, and consequently the College has a duty to provide students with quality Internet access as part of their learning experience. Given that they also use the Internet widely outside of school, students need to learn how to evaluate online information and to take care of their own safety and security as part of their broader education.
The purpose of Internet use in College is to raise educational standards, promote student achievement, develop initiative and independent learning, foster imagination and knowledge, support the professional work of staff and enhance the College's management functions.

2. Policy Aims

- To enable students to take full advantage of the educational opportunities provided by e-communication;
- To inform and educate students as to what constitutes appropriate and inappropriate Internet usage;
- To safeguard students and to protect them from cyber-bullying and abuse of any kind derived from e-sources;
- To help students take responsibility for their own online safety;
- To ensure that the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law;
- To help students use technology safely and appropriately.

3. Application to Staff Handbook

Staff should be ware that a further policy is contained in the Staff Handbook affecting the use of Internet for college purposes, entitled "ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY (Staff)".

4. DEFINITIONS

Cyberbullying is the deliberate use of information and communication technology (ICT), particularly mobile phones and the Internet, to hurt or upset someone else.
e-Safety means limiting the risks to which students are exposed when using technology, so that all technologies are used safely and securely.

5. GUIDELINES

Application
The College's e-Safety policy applies to all students. It is interpreted and applied age-appropriately.

Student responsibility
Students are responsible for their actions, conduct and behaviour when using the Internet, in the same way that they are responsible during classes or at other times in the working day.
Use of technology should be safe, responsible and legal. Any misuse of the Internet, inside or outside of school, will be dealt with under the College's policies. Sanctions will also be applied to any student found to be responsible for any material on his or her own or another website, Facebook, for instance, that would be a serious breach of College rules in any other context.

Bullying
Students must not use their own or the College's technology to bully others either inside or outside the confines of College buildings. Bullying incidents involving the use of technology will be dealt with under the College's anti-bullying policy.
If a student thinks s/he or another student has been bullied in this way, they should talk to their Curriculum Manager, Personal Tutor or Welfare Officer about it as soon as possible.

Abuse
If there is a suggestion that a pupil is at risk of abuse from his or her involvement on the Internet, the matter will be dealt with. If any student is worried about something that they have seen on the Internet, they must report it to their Curriculum Manager, Personal Tutor or Welfare Officer as soon as possible.

Responses
All e–safety complaints and incidents will be recorded by the College on the eSafety Incident Log, together with actions taken.

Breaches of regulations will be dealt with according to the College's disciplinary and child protection procedures.

Any instances of cyber-bullying will be treated in accordance with the College's anti-bullying policy and will be dealt with thoroughly and appropriately.

In such cases, the Principal will apply any sanction that is deemed appropriate and proportionate to the breach including, in the most serious cases, asking a student to leave the College.

6. PRINCIPLES AND ACCEPTABLE USE OF THE INTERNET

Monitoring and usage

Users should be aware that the College can track and record the sites visited and any searches made on the Internet by individual users.

We would advise parents that we provide filtered access to the Internet for students but they should also be aware that, with emerging and constantly changing technologies, there is no absolute guarantee that a student will not be able to access material that would be considered unsuitable. The chance of just coming across such content is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort an individual puts into their search.

Anyone inadvertently coming into contact with such material must contact a member of staff immediately.

When using the Internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity.

All College staff are expected to communicate in a professional manner consistent with the guidelines on the behaviour of staff in the education sector.

Access to the Internet in the College is given to students on the understanding that they will use it in a considerate and responsible manner. It may be withdrawn if acceptable standards of use are not maintained.

Staff should ensure that students know and understand that, in addition to the points found in the section on 'Online activities which are not permitted' below, no Internet user is permitted to:

- Retrieve, send, copy or display offensive messages or pictures;
- Use obscene or racist language;
- Harass, insult or attack others;
- Damage computers, computer systems or computer networks;
- Violate copyright laws;
- Use another user's password or account;
- Trespass in another user's folders, work or files;
- Use the network for commercial purposes;
- Download and install software or install hardware onto a College computer, whether legitimately licensed or not;

- Intentionally waste limited resources, including printer ink and paper;
- Use the school computer system or the Internet for private purposes unless the Principal/ Head has given express permission for that use.

Online activities which are not permitted in the College include:

- Copying, saving or redistributing copyright-protected material without approval;
- Subscribing to any services or ordering any goods or services unless specifically approved;
- Playing computer games unless specifically approved by the College;
- Using Internet chat rooms;
- Using the network in such a way that its use by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages);
- Publishing, sharing or distributing any personal information about any other user such as home address, email address, telephone number, etc);
- Using College computers or the Internet for financial gain, gambling, political purposes or advertising;
- Any activity that violates a College rule.

7. Managing email

Email is an immensely valuable tool for educational communication. However, it can also be a channel for cyber-bullying, abuse and defamation. Spam, phishing and virus attachments can also make email dangerous. As a consequence:

- Students must notify a member of staff if they receive offensive email;
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone not known to them without specific permission;
- Social email use during the school day can interfere with learning and will be discouraged;
- Sending or replying to anonymous messages and chain letters is not permitted;
- Staff should use College email accounts to communicate with students on professional matters only.

8. Managing Social Media and Social Networking sites

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow unmediated content to be published. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chatrooms, instant messaging and many others.

Students are advised never to give out personal details of any kind which may

identify them and / or their location. Examples include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs, etc.

Students are advised not to place personal photos on any social network space. They should think about how public the information is and consider using private areas.

Staff official blogs or wikis should be password protected. Staff are advised not to run social network spaces for pupil use on a personal basis.

Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed in how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.

Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Posts that, in the reasonable opinion of the College, could be deemed offensive or defamatory to individuals or to the College will be regarded as a serious breach of discipline and will be dealt with in the context of the College's behaviour policy.

9. Managing mobile phones

Students are permitted to bring mobile phones onto College premises but they remain the responsibility of their owners at all times. The College cannot be held responsible for any theft, loss of, or damage to, such phones suffered on College premises.

Students must not bring mobile phones into examinations under any circumstances

Phones may not be used to bully, harass or insult any other person inside or outside the College either through voice calls, texts, emails, still photographs or videos. Cyber-bullying of this nature will bring severe penalties in accordance with the College's behaviour policy.

Any misuse of the Internet through Internet-enabled phones, such as downloading inappropriate or offensive materials or posting inappropriate comments on social networking sites, will be dealt with in accordance with the College's behaviour policy.

Phones must not be used to take still photographs or videos of any person on College premises without their express permission. Even if such permission is obtained they must under no circumstances be used to ridicule, harass, bully or abuse another person in any way.

Any unacceptable use of mobile phones will be dealt with in accordance with the College's behaviour policy.

The College reserves the right to confiscate for a fixed period the phone of any

person contravening these protocols and to forbid them from bringing a mobile phone into College for any length of time deemed appropriate by the College.

10. Managing photography and video capture on College premises
Use of photographic material to harass, intimidate, ridicule or bully other students or staff members will not be tolerated and will constitute a serious breach of discipline.

Phones must not be used to take still photographs or videos of any person on College premises without their express permission. Even if such permission is obtained they must under no circumstances be used to ridicule, harass, bully or abuse another person in any way.

Indecent images taken and sent by mobile phones and other forms of technology (sometimes known as 'Sexting') is strictly forbidden by the College and in some circumstances may be seen as an offence under the Protection of Children Act 1978 and the Criminal Justice Act 1988. Anyone found in possession of such images or sending them will be dealt with by College authorities. If a student thinks that they have been the subject of 'sexting', they should talk to a member of staff about it as soon as possible.

The uploading onto social networking or video sharing sites (such as Facebook or YouTube) of images which in the reasonable opinion of the College may be considered offensive is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material. In this context it makes no difference whether the images were uploaded on a College computer or at a location outside of the College.

Students, if requested, must allow staff reasonable access to material stored on phones and must delete images if requested to do so in any situation where there is any suspicion such images contravene College regulations.

If the College has reasonable grounds to believe that a phone, camera, laptop or other device contains images, text messages or other material that may constitute evidence of criminal activity, the College reserves the right to submit such devices to the police for examination.

Such misuse of equipment will be dealt with according to the College behaviour policy and may involve confiscation and / or removal of the privilege of bringing such devices into College premises on a temporary or permanent basis.

11. Managing other electronic equipment – e.g. laptops, PDA's and tablet computers

Students are permitted to bring other electronic devices such as laptops, PDAs, tablet computers and mp3 players onto College premises with permission but they remain the responsibility of their owners at all times. They must keep them with them at all times or in a locked locker and they must ensure that they are appropriately made secure via passwords.

The College cannot be held responsible for any theft loss of, or damage to, such

phones suffered whilst at College. No electronic device should be misused in any way to bully, harass or intimidate another person whether through text or images. Any such abuse will be dealt with in accordance with the College's behaviour policy. No electronic device should contain inappropriate material such as violent or explicit videos or photographs, pornography or any material that could be considered offensive and / or inappropriate in a school context.

Anti-virus software - all laptops should have appropriate anti-virus software that is regularly updated.

Licensed software, distributing files / MP3's and Warez - no computer programs (executables), MP3's, pornography, or copyrighted material may be distributed over the network. This includes the sending of files via email, as well as setting up 'servers' on students laptops and using them as a means of sharing software. Also, students should not download copyrighted material or non-shareware programs and should not be using their laptops as a means to view films, images, or graphics which are deemed inappropriate.

Chatting - students may not use any chat or collaboration program to communicate with others through the College's computer network unless a teacher expressly permits them to do so. This includes the use of email during lessons.

Audio - because computer audio can be distracting, the volume setting on laptops must generally be turned off when used during school time.

Games – computer games should never be played in class or during study time.

Privacy – the College reserves the right to examine the hard drive on a student's personal laptop if there is reasonable suspicion that a computer is being used for inappropriate or dishonourable purposes.

College owned laptops / netbooks - these must only be used under the supervision of a member of staff and must only be used for educational purposes. The uploading of inappropriate material such as images, software and graphics is forbidden and this includes the doctoring of screen savers and backgrounds.

Consequences - students found in breach of these rules may have their Internet privileges removed, the privilege of using their laptop, netbook, PDA or tablet PC at College removed either permanently or temporarily, and, depending on the seriousness of the breach, they may also have other sanctions imposed in accordance with College's behaviour policy.

12. Responses to cyber-bullying

Cyber-bullying can be defined as "the use of Information Communication Technology, particularly mobile phones and the internet, deliberately to hurt or upset someone." (DCSF 2007)

Many young people and adults find using the Internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also be used

negatively. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyber-bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, College staff and parents and carers understand how cyber-bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

The DfE and Childnet have produced resources that can be used to give practical advice and guidance on cyber-bullying. See: http://www.digizen.org/cyberbullying

Cyber-bullying (along with all forms of bullying) will not be tolerated at Albemarle, whether the bullying originates inside or outside the College. Activities conducted outside of school premises and outside of school hours that in our opinion constitute cyber- bulling will also be covered by this policy. Instances of Cyber-bullying will be dealt with according to the College's anti-bullying policy. All incidents of cyber-bullying reported to the College will be recorded.

The College will take reasonable steps to identify the person(s) responsible for any instances of cyber-bullying such as examining system logs, identifying and interviewing possible witnesses and contacting the service provider and the Police if necessary.

Sanctions may include: Informing parents/guardians, the withdrawal of privileges e.g. to bring a phone into school or to use the College internet facilities, the person(s) responsible being instructed to remove any material deemed to be inappropriate, temporary or permanent exclusion in the most serious cases, and the Police being contacted if a criminal offence is suspected.

Reviewed Jan 2018