Caedmon College Whitby

E-Safety Policy

College Governance Status

This policy was created in June 2014 and was adopted by the Governing Body on 16 June 2014. It will be renewed every two years or in the light of new guidance or legislation.

Review dates	By Whom	Approval dates
Oct 2017	Staff and Governors	17.10.17
Sep 2019		

Signed by the Chair:

E-Safety Policy

Contents

1. Introduction

Caedmon College Whitby is a KS3/4/5 College catering for the educational needs of its students and preparing them for life after their tenure here. The College is extremely progressive in its approach to technology, to inform, educate and to facilitate learning to all users by utilising the best possible ICT equipment. This increasing development of ICT for curricular and administrative purposes is allowing students and staff to access a wider range of information more effectively and develop capabilities in the wide range of possibilities ICT can offer. This may be a student conducting research on the Internet, a member of administrative staff mail-merging letters from a database, members of the community accessing open-learning resources or a teacher analysing student performance, or parents accessing their child's record through E-portal or the Virtual Learning Environment (VLE).

2. Policy Statement

Caedmon College Whitby recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the College, while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training such as CEOP, guidance and implementation of our policies. Unfortunately, the likelihood of breaches of system integrity increases with the more frequent access to the network and the programmes contained therein. To safeguard learners and further the Every Child Matters agenda, we will do all that we can to make our learners

and staff E-safe and to satisfy our wider duty of care. This E-safety policy should be read alongside other relevant College policies and legislation.

3. Policy Scope

This policy applies to all users (staff, students and visitors) who have access to the College ICT systems and facilities, both on the premises and remotely. Any user of College ICT systems must adhere to and sign a hard copy of the E-Safety Policy. The E-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media sites which are connected in any way to the College.

4. Policy Review

The impact of the policy will be monitored regularly with a full review being carried out at least once a year. The policy will be reconsidered where particular concerns are raised or where an E-safety incident has been recorded.

5. Roles and Responsibilities

All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. When informed about an E-safety incident, staff members must take particular care to emphasise that although confidentiality will be maintained it will be passed to the relevant member of staff, as a matter of priority.

Designated Safeguarding Lead

There are clear lines of responsibility for E-safety within the College. The first point of contact is the **Designated Safeguarding Lead: (**dsl@ccwhitby.org) who is Mr Jonathan Bond (JJB), responsible for Child Protection and Safeguarding. He will decide the most appropriate course of action to take and which department or agency should be involved (eg, if it is a case of cyber-bullying then the Network Manager may be required to collate evidence).

All learners must know what to do and who to contact if they have any E-safety concerns. In most cases, this will be a member of staff. A confidential email address has also been set up to report incidences of bullying. Should any incident occur that relates to E-safety, this will be investigated and the evidence will be collected; relevant external agencies (eg, NYP) will be informed as necessary.

E-Safety Officer

The E Safety Officer is responsible for the implementation of policies designed to encourage a positive approach to E Safety. The designated officer responsible for E-Safety is Mr Andrew Whelan. To assist him the Network Manager and ICT team are responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will be expected to be at the forefront of any matters pertaining to E-Safety, review and update the E-Safety Policy, deliver staff training, record incidents, report any developments and incidents to the Officer responsible for Child Protection at the College. Nominated ICT personnel are to liaise with the Local Authority and external agencies to promote E-safety within the College community. They may also be required to deliver workshops for parents.

Students

Students are responsible for using the College ICT systems and mobile devices in accordance with the guidelines set out in students' planners, which are signed at the time of registration by students and parents. Students are expected to act safely and responsibly at all times when using the internet and/or mobile technologies. They are responsible for attending E-safety lessons as part of the curriculum and are expected to know and adhere to other relevant College policies, eg, those regarding the use of mobile phones, images, cyber-bullying, etc. They must follow the reporting procedures where they are worried or concerned, or where they believe an E-safety incident has taken place involving him/her or another member of the College community

Sanctions

Violation of the above rules will result in a temporary or permanent ban on unsupervised use of College computers. Violation of the above rules will result in a temporary or permanent ban on Internet access on the College network. Violation of the rules outlined in 'Students access to the internet' will result in a temporary or permanent ban on Internet access on the College network. Additional disciplinary action may be added in the line with existing practice depending upon severity of misuse. When applicable, police or local authorities may be involved.

Age appropriate information should be given every academic year to every student in Caedmon College Whitby.

Parents

Parents will be offered training and support to ensure their child remains safe. This will be offered at **all** parents' evenings and other additional parent's events. Parents can also contact the College through their Anti-Bullying website and or by using the dedicated Anti-Bullying Phone Number – 07790 428 584

Staff

All staff are responsible for using College ICT systems and mobile devices in accordance with the College computing policies, which they must sign and records will be kept by an appropriate College Officer in this respect. Staff are responsible for attending training on E-safety and displaying a model example to learners at all times through embedded good practice. All digital communications with learners must be professional at all times and be carried out in line with the Acceptable Use Agreement – ICT and E-Technology Policy. Online communications with learners are restricted to the College network and College Twitter accounts. External platforms, not hosted by the College, such as social media sites, should not be used to communicate directly with students. Any incident that is reported to or discovered by a staff member must be reported to the designated officer responsible for E-Safety and/or their line manager, without delay.

6. Security

The College will do all that it can to make sure that all users of its systems are protected by keeping the College network safe and secure. Data is shared to external sites to facilitate Google Classroom and other systems for the management of classroom data, e mail etc. This is in accordance with current Data Protection legislation. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of web-filtering and protection by firewalls. Physical protection of data held on servers and workstations to prevent accidental or malicious access of College systems and information will include access controls to hardware (such as password protection and encryption of drives as required). Data held on servers will be restricted by access permissions so that only relevant parties have access. This will be controlled by the ICT department. All staff are expected to have their USB drives encrypted either through hardware (or as hardware

encryption is cost prohibitive), or software encryption programs (Bit-locker is available on all College computers). Digital communications, including email and internet postings, using the College network, will be monitored in line with the email and social media policies available from the College's I:Drive and the College website. Staff should ensure their user areas, data and emails are not left available for unauthorised access by securing/locking their machines when unattended. Data copied to personal devices (eg, emails on mobile telephones) must not be made available to unauthorised users and these devices must be secured with security unlock codes. By staff signing this policy or students and their parents signing the student log books / planners users are accepting that the college ICT dept will routinely monitor users' internet and ICT usage using college facilities.

7. Behaviour

Caedmon College Whitby will ensure that all users of technologies adhere to the standard of behaviour as set out in the Staff Computing, Acceptable Use, Email and Internet Policies and any other relevant policies), accessible from the College's I:Drive and the College website. The student rules for the use of ICT and related facilities is set out in student planners. The College will not tolerate abuse of ICT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes and policies contained in policies in the College's I:Drive/the College website and in student planners. Where conduct is found to be unacceptable, the College will deal with the matter in accordance with agreed disciplinary procedures. Where conduct is considered illegal, the College will report the matter to the police.

8. Communications

Caedmon College Whitby requires all users of ICT to adhere to the relevant policies contained on the I:Drive and on the College website, or in the student rules for the use of ICT and related facilities in student planners, for communications between staff and students. Emails from students to individual staff members should normally use the generic College email address: Post@ccwhitby.org, with a clear identifier for the staff member concerned. Staff should normally only use the College email address for students, eg, 123456@ccwhitby.org through approved email groups involving other staff (eg, digitalleaders@ccwhitby.org) or by using the VLE where there is transparency and monitoring by the system administrators. For College Twitter accounts, staff are not to enter into individual dialogue or non-curriculum discussions with students.

9. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (eg, images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or students.

All students and staff should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example. Images or videos that are downloaded or uploaded on College ICT equipment, whether for personal use or as part of learning, should not be offensive, pornographic, inflammatory or in any way bring the College into disrepute. Images or videos of staff or students should not be used without consent and student images should not normally identify the student, unless parental permission is sought. Photographs of activities on the College premises should be considered carefully and have the consent of the Principal, and the parties involved, before being published. Any images of students taken on private devices for official purposes only should be deleted as soon as they are uploaded to the appropriate College network.

10. Personal Information

Any processing of personal information needs to be done in compliance with the Data Protection Act 1998. This is likely to include content such as student records, e-portfolios and assessed work. Caedmon College Whitby is legally obliged to take steps to minimise the risk that data will be lost and processed unfairly.

Personal identifiable information is information about a particular living person that can identify them to the reader. Caedmon College Whitby collects and stores the personal information of students and staff regularly to conduct its business (eg, names, dates of birth, email addresses, assessed materials and so on). The College will keep this information safe and secure and will not share it without the express permission of the parent/carer, unless appropriate external organisations, eg, the Local Authority or police require this for specific, legitimate purposes; this will be with the permission of the Principal.

No personal information should be posted on the College website without the permission of the Principal. Only names and work email addresses of (senior) staff should appear on the College website. Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Staff should have clear and definable reasons for having any personal data off-site and the permission of the Principal. Every user of College ICT facilities is expected to log off or secure their PC or laptop on completion of an activity, or where they intend to be physically absent from a device for any period. All College mobile devices such as laptops, chrome-books, tablets and mobile telephones are required to be password protected, USB drives are to be encrypted either by built in hardware or encryption software (Bit-Locker) before leaving the premises. Where the personal data is no longer required, it should be securely deleted.

11. Education and Training

With the current unlimited nature of internet access, it is impossible for Caedmon College Whitby to eliminate all risks for staff and students. It is our view therefore, that the College should support staff and students stay E-safe through regular training and education. This will provide individuals with appropriate skills to be able to identify risks independently and manage them effectively.

For Students

Students will attend e-safety lessons in PHSE sessions as well as receiving CEOP training. The first of these sessions will take place at the beginning of the new College year with follow up lesson(s) carried out termly. Issues associated with E-safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Students should also know what to do and who to talk to if they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. A link to the College E-safety guidance will appear when users log on to the College website and this guidance will be highlighted in posters and leaflets around the College as well as on the E-safety area of the College's VLE. In classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will be encouraged to respect the copyright of other parties and to cite references correctly.

For staff

Staff will take part in mandatory E-safety training at the start of the new College year through CPD sessions. This will be led by the designated person for E-safety and undertaken by relevant staff.

This will normally take the format of workshops, allowing teachers hands-on experience. Further resources of useful guidance and information will be made available to staff through the VLE and in regular bulletins. Each member of staff must sign to indicate they have received the training and these records will be retained in College. Any new or temporary staff will receive training on the College's ICT system, provided by ICT department staff. They will also be asked to sign the College (staff) Acceptable Use Policy and E-Safety Rules.

12. Incidents and Responses

Where an E-safety incident is reported to the College, this matter will be dealt with very seriously and with urgency. Caedmon College Whitby will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their form tutor, or via an email to an appropriate member of staff. Where a member of staff wishes to report an incident, they should contact their line manager or the member of staff designated responsible for E-safety, as soon as possible. Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the College Acceptable Use Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

13. Feedback and Further Information

Caedmon College Whitby welcomes constructive feedback on this and any other College policy. If you would like further information on E-safety, or wish to send us your comments on our E-Safety Policy, please contact Mr Jonathan Bond or Mr Andrew Whelan (Email: post@ccwhitby.org, telephone: 01947 602406).

✂

Caedmon College Whitby E-Safety Policy User Agreement

To: The Principal

Name: …… (Member of staff)

I have read the 'Caedmon College Whitby E-Safety Policy' and agree to its contents.

Signature: ..... (Member of staff) Date: ……