The Chalfonts Community College

October 2018

Review Date : October 2019

Member of Leadership responsible : Vice Principal (Inclusion/Pastoral)

E-SAFETY POLICY

The Chalfonts Community College

E-Safety Policy

1. Introduction

The internet and digital communications are essential elements of 21st century life for education, business and social interaction. The college has a duty to provide students with high quality access and technologies as part of their learning experience and also to educate them in its appropriate use. This e-safety policy covers issues relating to students, teachers, parents and other adults and their safe use of the internet and other mobile communication technologies.

2. Aims

- To safeguard children, young people and staff
- To educate and empower children so that they possess the necessary skills to make safe and responsible decisions and feel confident to report any concerns they may have
- To raise awareness of the importance of e-safety amongst all staff so they are able to educate and protect students in their care
- To inform staff how to manage their own professional reputation online and demonstrate appropriate behaviour compatible with their role

3. Acceptable use of Curriculum Network, Internet, Email and Online Systems

The college network, email and online systems are operated by the college and made available to staff and students at the discretion of the college. No user is entitled to use of the systems and gross misuse will result in denial of access, and, in some cases, disciplinary action and exclusion. The statement has been drawn up to protect all parties.

The college reserves the right to examine and delete any files held on the system, to monitor any Internet sites visited and email sent between students.
All of this is in accordance with Data Protection, Laws of Copyright and the Education and Inspections Act 2006 (EIA 2006).

Network, Internet and Email

Use of the Internet & email by staff & students is permitted and encouraged where such use is suitable for education purposes and supports the goals and objectives of the college. The Internet & email is to be used in a manner that is consistent with the College's standards of conduct. College email accounts are to be used for college and education purposes only.

However, limited personal use is considered acceptable. User account access should only be made via the authorised account and password by the assigned student. The college reserves the right to directly access students' network and email accounts in the pursuit of an appropriately authorised legal or disciplinary investigation. The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately (the Police have right of access to recorded data in pursuit of a crime). Use of the internet and email may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.

The distribution of any information on the college's network is subject to the scrutiny of the College, who reserve the right to determine the suitability of this information.
The use of email attachments within messages is strictly limited to professional and educational purposes only. Users found to be sending unfit email attachments may be subject to having their privilege to use the system revoked and could result in disciplinary action. Abuse towards other users via email and forwarding chain letters is forbidden.

Use of the network to access and publish inappropriate content such as pornography or racist material anything of an offensive nature is strictly forbidden. This could result in disciplinary action and exclusion taking place.

Copyright of materials must be respected and acts of plagiarism are strictly prohibited. Network equipment and resources provided to students by the college must be respected and any problems must be reported to the IT support team.

Students must not share account passwords or allow other students usage of their account, as account responsibility lies with the student whom the account has been assigned to; this includes network usage, internet browsing, email sending and equipment usage such as printing.

4. Cyber-bullying

The College community has a duty to protect all its members and provide a safe and healthy environment to work in.

Students are advised to never reveal any personal information about themselves or anyone else (for example: email address, personal websites/blogs, mobile number, telephone number or home address). The use of Information Communication Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else is prohibited.

The Principal has the power "to such an extent as is reasonable" to regulate the conduct of pupils when they are offsite. This is significant in cyber bullying which often takes place out of school but can impact very strongly on the school life of those pupils involved.

Confiscation of mobile phones when they are being used without permission in class or used to bully is included within the act. Cyber bullying can be a criminal offence under the Protection from Harassment Act 1997, Communications Act 2003 and the Public Order Act 1986. The age of criminal responsibility in the UK starts at 10 years old.

Students are instructed to not retaliate or reply to someone who is bullying them. They should save the evidence or, if necessary, learn how to keep records of offending messages or pictures and contact a member of staff if they need advice.

5. Policy of Mobile Phones

The use of mobile phones in school is not permitted. If a student has to get an urgent message home they can do so through our Reception staff. If a parent needs to get an urgent message to their child, this can also be done through our Reception office. Mobile telephones are banned in examinations and need to be handed in to the numbered plastic wallet provided. Failure to do so may result in disqualification from that examination.

If a mobile telephone/ iPod is brought into College the following must be followed:

• They must be switched off at all times including breaks, during lessons, and on the way to lessons unless they are instructed to use them by a teacher.

• No photographs or videos are to be taken at any time, including on College transport without the consent of the students or staff involved.

• They must not be used to send unpleasant texts or pictures/images which will be regarded as cyber bullying

Students who fail to comply with these requirements will have their mobile phones confiscated, and returned at the end of the day, in the first instance. Any further misuse will require parents/guardians to collect the phone after school and may result in the phone being confiscated for extended periods of time.

In instances of cyber-bullying or online abuse, parents will be contacted and required to attend a meeting with one of the Designated Safeguarding Officers. It may be deemed in certain cases that the police need to be informed.

Mobile phones/iPods can be searched, without parental consent, if we believe that the phone is used in a disruptive, bullying or unsafe way.

The College will not accept responsibility for mobile telephones at any time and will not investigate any loss. We recommend that that parents take out their own insurance to cover any loss, theft or damage.

We reserve the right to ban mobile telephones at short notice for any group of students or individuals who fail to adhere to this policy.

6. Virtual Learning Environment (Google Classroom / Moodle)

The sole purpose of the Chalfonts Community College's Virtual Learning Environment is to deliver electronic learning. This "Responsible Use" statement will help protect pupils, staff and the school by clearly stating what is acceptable and what is not.

Contributions must be civil and respectful. No disruptive, offensive or abusive behaviour will be tolerated; contributions must be constructive and polite, not disrespectful or contributed with the intention of causing trouble.

All students are advised to “Think before you send” as whatever is sent can be made public very quickly and could stay online forever. Any content which is unlawful, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented, racially offensive or otherwise objectionable material is not acceptable.

Parents/carers of all students will be asked to read and sign an ICT Acceptable Use Policy (Appendix 1) before their child’s account is created.

Staff are expected to be familiar with both the ICT code of practice (Appendix 2) and the guidelines for use of internet based social networking.

7. Educating parents and students

E-safety updates and advice are shared with parents at information evenings throughout the academic year. Parents are advised on the best ways of ensuring that their child’s online activities are safe.

Students are advised on online safety through a variety of channels: PSHCE lessons, assemblies, ICT lessons. Mobile phone rules are regularly reinforced.

8. Linked policies

- Behaviour
- Safeguarding/Child Protection
- Anti-bullying

APPENDIX ONE

THE CHALFONTS COMMUNITY COLLEGE
STUDENTS' USE OF ICT SYSTEMS AND INTERNET

STUDENT AGREEMENT

1. **Network Access and Passwords**

- I will take care of all ICT equipment that I use.
- I will never give my password to anyone, even my best friend. If I think someone has obtained my password, I will report this to my teacher immediately and change it.
- I will not attempt to gain unauthorised access to the Chalfonts Community College network or to any other computer system found on the internet. I will not attempt to logon using another person's username and password, or to access another person's files.
- I will only use the network for College work and homework. My teacher, or network manager, may check the content of my files.

2. **Internet and Websites**

- I understand that my teacher and the Internet service provider will monitor the sites I have visited and may check the content of any email, or other message that I have sent.
- I will not use the Internet to view inappropriate material (such as racist or pornographic sites). If I am unsure if a site is suitable, I will ask a member of staff before attempting to access the site.
- I understand that information on the Internet may not always be reliable and sources may need checking.
- I will not take information from the Internet and pass it off as my own work.

3. **Email and other forms of electronic communication**

- I will always use email in a responsible and appropriate manner.
- I will only send and respond to emails from people I know, or that a teacher has approved.
- I will not send or respond to nasty, suggestive or rude emails or messages via bulletin boards.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I will never send anyone my picture, or that of another person without permission from my teacher/parent/guardian/carer.
- I am not allowed to send large volume emails (spamming).
- I will never tell anyone I communicate with on the Internet my home address, my telephone number, my College's name, or arrange to meet anyone I communicate with on the Internet in person.
- I am not allowed to use an Internet chat room.
- I will inform the teacher of any misuse of the internet, or email that comes to my attention.

I have read this policy and agree to follow it. I understand that disciplinary action may be taken and my Internet access may be removed if I misuse email, or the Internet and my parents/guardian will be informed.

Student's Name ……..

Signed Student ……..

APPENDIX TWO

The Chalfonts Community College

Staff Use of ICT Systems, Internet Policy and Code of Practice Agreement

1. Important ICT Policy - To keep you safe

You are expected to follow the schools policy when using any equipment or accessing the internet.

Network Access and Passwords

- Keep your password secure - do not share.
- It is your responsibility to prevent your User ID and Password being used by others to gain access to IT equipment at the College.
- It is a breach to attempt to access unauthorised areas including attempting to login to another person's area.
- Computer screens **must** be locked to prevent unauthorised access when unattended.

2. Internet Safe Practice

- It is an offence to attempt to use equipment to access unsuitable websites of an inappropriate nature including adult material, racist or indecent sites.
- Be aware that we will routinely monitor sites and material viewed on school property.
- Adhere to copyright laws and no plagiarism.

3. Email

- Use email responsibly and ensure all messages are polite, respectful and appropriate about individuals/ the college.
- Sending images of students or staff is prohibited without written permission.
- Personal external email accounts should never be used in conversations between staff/students and parents.
- Staff must report any inappropriate email correspondence from or with a student to Principal - inappropriate emails from staff or parents report directly to Principal.
- Staff can only engage in VLE forums. Other networking and chat site facilities with students is prohibited.
- The Vice Principal and network manager may access staff email if they believe inappropriate use.

4. General

- Staff may only keep information about students which is in line with the data protection legislation. Any shared information to outside parties must be sanctioned by a member of SLT.
- Content of staff files may be checked by the network manager at any time, with the permission of the Principal, if there are concerns.
- Staff must follow the procedure regarding ICT systems in the staff handbook.
- The college will cooperate with any appropriate officials, or police, in any investigation related to potentially illegal activities conducted in the college.

5. Loan of equipment

- Written permission from parents is required for loan of IT equipment to students outside of school.

- School equipment, if taken off site should only be used for work related activity.

6. Staff enforcement and monitoring of the Student ICT Policy

Staff must enforce and monitor ICT Policy at all times, in particular:

- If students deliberately or accidently access unsuitable materials staff should make note of student, pc and sit/material accessed.

- Staff should monitor and scrutinize what students are accessing.

- Staff should provide clear guideline for content of email messages, sending and receiving procedures.

- Staff should provide students with skills and techniques to enable efficient and effective use of the internet and seek opportunities to educate about safe practices.

- Staff should ensure students have clearly defined learning focus for using the internet and email.

- Staff should ensure that students only access the College network using approved College ICT equipment and do not allow students access to the PC/laptops allocated for teacher use.

- If you fail in your duty of care to protect yourself and the school by allowing students to access staff computers, or work areas, this will be considered to be gross misconduct and will be subject to the College's disciplinary procedures. Failure to adhere to this may result in summary dismissal.

Member of Staff's name …….

Member of Staffs signature …….