E-Safety Policy

Introduction

1. Chapeltown Academy recognises the benefits and opportunities which new technologies offer to teaching and learning. The Academy provides internet access to all students and staff and encourages the use of technologies in order to enhance skills, promote achievement and enable lifelong learning.
2. Notwithstanding paragraph 1 above, the accessibility and global nature of the internet and different technologies available mean that the Academy recognises potential risks and challenges associated with such use.
3. The Academy's approach is to implement appropriate safeguards within the environment while supporting staff and students to identify and manage risks independently and with confidence. This can be done through combining appropriate security measures, training, guidance and implementation of policies.
4. In furtherance of our obligation to safeguard students we will do our utmost to ensure students and staff stay e-safe.
5. This e-safety policy should be read alongside other relevant policies (e.g. Safeguarding and Child Protection, Teaching and Learning etc.)

Creation, Monitoring and Review

6. The Academy's policy on e-safety will be monitored regularly with a full review being carried out regularly by the Governing Body. This will include a review of whether the Academy will adopt a "bring-your-own device" policy.
7. The Senior Leadership Team and the Student Executive will discuss the Academy's e-safety policy annually and make recommendations to the Governing Body ahead of its annual review.

Scope

8. The policy applies to all members of the Academy's community who have access to the Academy's ICT systems, **both on the premises and remotely.**
9. Any user of the Academy's ICT systems must adhere to and sign a copy of the Acceptable Use Policy which includes a specific section on e-safety. This Acceptable Use Policy is included as an Appendix to this policy.

10. The e-safety policy applies to all use of the internet and forms of electronic communication, including e-mail, mobile phones and social media sites.

Responsibilities

11. There are clear lines of responsibility for e-safety within the Academy. Overall management of the e-safety policy and procedures lies with the Safeguarding Officer, Mr Ali Jaffer.
12. All staff are responsible for ensuring the safety of students and should report any concerns immediately to their line manager.
13. The teaching of e-safety to students is part of the student induction process. Teachers should ensure their day-to-day teaching complies with the principles of e-safety as described in this policy.
14. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.
15. All students must report e-safety concerns to either their Form Tutor or Mr Ali Jaffer, the Safeguarding Officer, or Amanda Southworth, Deputy Safeguarding Officer.
16. Where any report of an e-safety incident is made, all parties should understand the procedure and how this will be followed up. In cases where it is appropriate, the Safeguarding Officer may be asked to intervene with additional support from external agencies.

Security and Risk Assessment

17. The Academy will do all that it can to make sure its network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of the Academy's systems and information.
18. Digital communications, including email and internet postings, over the Academy's network, will be monitored in line with the statement of acceptable use of ICT.
19. In making use of new technologies and staff are advised to carry out a risk assessment for e-safety which should include recording of evidence of risks and countermeasures.

Behaviour

20. The Academy will not tolerate any abuse of ICT systems.
21. The Academy will not tolerate communication which is not respectful (whether initiated by staff or students).
22. Any reported incident of bullying, harassment or other unacceptable conduct will be treated seriously and in line with the relevant disciplinary codes.
23. Where conduct is found to be unacceptable, the Academy will deal with the matter internally.
24. Where conduct is both unacceptable and illegal, the Academy will report the matter to the police.

Communication

25. Communication between students and adults (including parents, mentors and other external parties), by whatever method, should take place within clear professional boundaries.
26. The responsible use of social media may be encouraged for educational purposes so long as clear professional boundaries are maintained.
    a Staff are not to use their personal social media accounts to follow/like/befriend/retweet/favourite or interact with current students or their statuses or postings on Twitter, Facebook or Instagram
    b Staff may have professional Twitter accounts but these must be specifically sanctioned by the Senior Leadership Team
    c Other social media must be used thoughtfully and responsibly
    d Any social relationships/interactions via social media with former students must remain professional
27. Staff must use their own official *@chapeltownacademy.com* email address when communicating with students via e-mail, unless exceptional circumstances apply.
28. As a reminder all internet and e-mail activity is actively monitored and investigations could take place on request of the Head Teacher or the Governing Body.
29. Unacceptable failure to comply with the communication protocols described above in will be dealt with internally. Where such unacceptable failure has resulted in communication which is illegal, the matter will be reported to the police.

Use of Images and Video

30. The use of images is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. other intellectual property or data protection rights).
31. All students and staff should receive training on the risks when taking, downloading and posting images online and making them available to others.
32. Informed consent should be sought from all relevant part(y)(ies) before an image is taken or shared.
33. Agreements should be in place as to whether images are to be destroyed or retained for further use and in the case of the latter where these are stored and who will have access to them.
34. Due regard must be had to the principles of the Data Protection Act and the Academy's Data Protection Policy.
35. Photographs of activities on the Academy's premises should be considered carefully and have the consent of a member of the Academy's Senior Leadership Team before being published.
36. Particular care should be taken when images are taken where students can be individually identified.

Personal Information

37. The Academy collects and stores the personal information of students and staff regularly e.g. names, dates of birth, email addresses, assessed materials and so forth. The Academy will keep that information safe and secure and will not pass it onto anyone else without the express permission of the student/parent/ carer.

38. No personal information can be posted to the Academy's website unless such an action complies with the Academy's Data Protection Policy.

39. Only names and work email addresses of staff will appear on the Academy's website. Personal information will not be available without the consent of the relevant party.

40. Staff must keep students' personal information safe and secure. It is good practice to ensure all personal information is password protected.

41. Where the Academy's mobile devices (e.g. laptops, USB devices etc.) are taken off the premises, security is paramount. Staff should ensure they are password protected.

42. Where the personal data is no longer required, it must be securely deleted in line with the Academy's Data Protection policy

Education and Training

43. With the current unlimited nature of internet access, it is impossible for the Academy to eliminate all risks for staff and students. The Academy should, therefore provide individuals with the skills to be able to identify risks independently and manage them effectively.

44. Students will receive an e-safety briefing during the Academy's induction period.

45. Issues associated with e-safety apply across the curriculum and students should receive guidance on appropriate precautions and safeguards when using internet and technologies.

46. Staff will take part in mandatory e-safety training (as part of their safeguarding training) before the start of a new academic year. Further resources will be issued to staff following the session.

47. Every member of staff must record the date of the training attended on their CPD log.

48. New and temporary users will receive training on the Academy's ICT system, led by the e-safety officer. They will also be asked to the sign the Academy's Acceptable Use Policy.

49. Staff are reminded that section 16 of the Sexual Offences Act provides that it is an offence for a person aged 17 or over to have a sexual relationship with a child under 18 where that person is in a position of trust in respect of that child, even if that relationship is consensual.

Incidents and Response

49. Where an e-safety incident is reported to the Academy this matter will be dealt with seriously. The Academy will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

50. If a student wishes to report an incident, they can do so to their Form Tutor or to the Academy's Safeguarding Officer, Ali Jaffer.

51. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, the Academy will review what has happened and decide on the most appropriate and proportionate course of action.

52. 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.

Feedback and Further Information

53. The Academy welcomes all constructive feedback on this and any other of the Academy's policies. If you would like further information on e-safety or you wish to send us your comments on this policy, please contact: Ali Jaffer via contact@chapeltownacademy.com

Appendix 1 to the E-Safety Policy Statement of Acceptable Use

General Principles

1. This acceptable use statement is applicable to students, staff and anybody who uses the Academy's ICT hardware, software or network.
2. For the purposes of this document the "Internet" is defined as including web services, chat rooms, bulletin boards, newsgroups, peer to peer file sharing and instant messaging software
3. Use of the Internet is permitted and encouraged where such use supports the goals and objectives of the Academy.
4. Use of the Internet is monitored for security and/network management reasons
5. Users may be subject to limitations on their use of such resources
6. Unacceptable behaviour includes, but is not limited to
    a. Visiting websites that contain obscene, hateful or other objectionable materials
    b. Making or posting indecent remarks, proposals or materials on the Internet including discriminatory jokes and defamatory comments
    c. Downloading software or other electronic files without the use of virus protection measures that have been installed by a member of ICT support
    d. Intentionally interfering with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network
7. Users should
    a. Raise any security breaches (e.g. unauthorised access to accounts) with a member of the Senior Leadership Team
    b. Record any instances where inappropriate sites have been accessed by accident
    c. Utilise Remote Desktop connections and/or secure learning systems when accessing personal information relating to students and members of staff

E-mail

8. The Academy's email accounts are to be used for the Academy's business. Personal use is not encouraged and must be limited.

9. Use of email may be subject to monitoring for security and/or network management reasons
10. Email messages are treated as corporate messages of the Academy.
11. The Academy reserves the right to redirect the email sent to staff email accounts that have left the Academy, where the purpose is a legitimate business or professional purpose.
12. Unacceptable behaviour includes, but is not limited to
    a. Soliciting emails that are unrelated to the Academy's activities or for personal gain
    b. Sending or receiving any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
    c. Uploading, downloading or otherwise transmitting commercial software or any copyrighted materials belonging to parties outside of the Academy or the Academy itself.
    d. Wasting time on non-Academy related matters
13. Users should
    a. Archive effectively
    b. Never reply to spam
    c. Draft communications with care
    d. Re-read messages before sending to check for clarity and ensure they contain no information which may put the school at unnecessary risk
    e. Effectively use the CC and BCC
14. The Academy maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation

I ___, agree to abide by the above statement of acceptable use and understand that if I breach these rules I will be subject to a disciplinary procedure which may involve withdrawal of ICT access and/or other sanctions.

Name: _____ *Position:* _____ *Date:* _____

In the case of students : Parent/Guardian Signature _____

Signed by *SRuston* & *DNicholson*

Agreed by TGB – April 2014

Reviewed by	Governing Body
Last Reviewed	November 2016
Adopted by TGB	April 2014
Next Review	November 2017