



Computer, Email and Internet Policy

Centre Academy London

Implementation date: 1st September 2022

Next review date: 1st September 2023

Signed:

Date: 01/09/2022

A handwritten signature in black ink, appearing to read 'Kas Lee-Douglas'.

Mrs Kas Lee-Douglas
Head of School

Signed:

A handwritten signature in black ink, appearing to read 'Samina Yar', positioned above a blue horizontal line.

Date: 01/09/22

Mrs Samina Yar



1. Introduction

Centre Academy London (CA London) knows that technology can enhance education and help children access learning and fulfil their potential. The school also recognises its duty of care and its responsibility to safeguard both students and staff.

CA London provides various technology for use by staff and students. In addition, mobile devices are increasingly common, and internet enabled equipment is likely to be brought to school by staff, students and visitors. Due to this ease of access, it is important for the school to establish policies to ensure that technology is used appropriately and effectively, and the associated risks are reduced. These risks are classified in The Byron Review (Safer Children in a Digital World, 2008). They may be from content, contact or conduct and are often determined by behaviours. A full list of risks is not included here but includes:

- Adverts, spam, sponsorship
- Personal Information
- Violent/hateful content
- Pornographic or unwelcome sexual content
- Bias, racist and/or misleading information/advice
- Being cyber bullied, bullied, harassed, sexually harassed or stalked
- Being groomed or meeting strangers
- Self-harm
- Illegal downloading
- Hacking
- Gambling
- Terrorism
- Creating and uploading inappropriate material, and images
- Providing misleading information/advice

The school takes an educational approach to digital safety in order to equip students with the skills and knowledge they need to use technology safely and responsibly. It is important life skill for students to know how to stay safe and is able to manage online risks.

The policy will be reviewed and updated regularly. It applies to staff, students and visitors to CA London.

1.1 Contents

1. Introduction	1
1.1 Contents	2
2. Equipment	3
2.1 All Users	3
2.2 All Students	4
3. Security and privacy	4



4. Internet.....	4
5. Email.....	5
6. Mobile Devices.....	5
7. Enforcement.....	5
7.1 Students.....	6
7.2 Staff.....	6
7.3 Parents.....	5
8. Principles for acceptable use of the Internet.....	6
8.1 All Staff and Students.....	6
8.2 Staff.....	7
9. Responsibilities.....	7
9.1 The School.....	7
9.2 Students.....	7
9.3 Staff.....	7
9.4 Parents.....	7
10. Useful Websites.....	8
Appendix 1 – Summary of Rules.....	9
Appendix 2.1 – Student Signature Sheet.....	10
Appendix 2.2 – Staff/Visitor Signature Sheet.....	11

2. Equipment

Computers and internet access are provided and maintained for the benefit of all staff and students, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour on the Internet just as they are responsible for their behaviour in a classroom or a corridor. Students should remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

2.1 All Users

The following rules apply to staff, students and visitors using School provided ICT equipment, including desktops and laptops:

- Do **NOT** install, attempt to install or store programs of any type on the computers without permission.
- Do **NOT** damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do **NOT** use the computers for commercial purposes, e.g. buying or selling goods unless authorised by Mrs Yar and Mrs Lee-Douglas.
- Do **NOT** open files brought in on removable media (such CDs, DVDs, USB drives etc.) until they have been checked with antivirus software, and been found to be free of viruses.
- Students and visitors should **NOT** connect equipment to the network. Staff may connect School equipment and personal devices to the network; however, they



should ensure that School internet usage rules are followed even on personal devices.

- Do **NOT** eat or drink near computer equipment.
- All faults, failures and breakages must be reported to **Mrs Yar** or to a teacher.

2.2 All Students

In addition, the following rules apply to students:

- Students must follow instructions regarding usage of mobile devices.
- Students may **NOT** use laptops or computers during breaktime or lunchtime.
- Students may **NOT** take School equipment home.

3. Security and privacy

The security and privacy rules below apply to all staff, students and parents. In addition, there is a separate staff policy on the security of personal data.

- Do **NOT** disclose your password to others, or use passwords intended for the use of others.
- Do **NOT** use the computers in a way that harasses, harms, offends or insults others.
- Do **NOT** use personal emails and other communication platforms.
- Respect, and do **NOT** attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and memory sticks brought to School may be reviewed and communications checked to ensure that users are using the system responsibly.

4. Internet

The follow rules are in place for all staff, students and visitors using the School network.

- The Internet should only be used for study or for School authorised/supervised activities.
- Do **NOT** use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the School, as well as other pupils or staff. This includes abiding by copyright laws.
- Do **NOT** engage in 'chat' activities over the Internet e.g. use Discord or other chat rooms.
- Do **NOT** take pictures of any persons in school and share it without their permission.
- In addition, students need to be aware that they should **NOT** arrange to meet anyone via the Internet. People they contact online are **NOT** always whom they seem.



5. Email

The following rules apply to all students, staff and visitors. They apply to email as well as other forms of electronic communication.

- Students and staff will only use their School email address.
- Students and staff are all provided with individual accounts for email and document storage. These must be used appropriately.
- Be polite and appreciate that other users might have different views from your own. **The use of inappropriate language, swearing or intimidating behaviour is NOT allowed.**
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which could destroy information and software on the computers/network.
- The sending or receiving of emails or information containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Any students receiving such messages should report this immediately to a member of staff.

6. Mobile Devices

The following rules should be read in conjunction with the relevant sections in the Student Handbook, Parent/Carer Handbook or Staff Handbook.

- The school takes no responsibility for mobile devices brought to the School by staff, students or visitors.
- Students must not bring mobile devices to school except mobile phones with parent/carers permission. The only exception to this are devices needed for specific lessons, in which case, they should be treated as mobile phones and handed into mentors during mentor time.
- **Student mobile phones must be switched off when students enter the yard in the morning.**
- **Student mobile phones should be handed in to mentors on entry to school, or the School Office if permission has been given for lunchtime off-site privilege mobile phone usage or if they are late to school.**
- **Student mobile phones should be collected from mentors at the end of the day and must not be switched on until students have left School premises.**

7. Enforcement

This document is to be read carefully by all staff and pupils. A copy will be issued to each staff member and pupil, and this must be signed and returned to the School. If any pupil or staff member violates these provisions, access to the Internet will be denied and disciplinary action will be taken. Where appropriate, the police may be involved or other legal action taken.



7.1 Students

For students, additional action may be taken by the School in line with the School's Promoting Good Behaviour and Discipline Policy. For serious violations, students may be excluded.

7.2 Staff

For staff, action may be taken under the School's Disciplinary Policy.

7.3 Parents

For parents, action may be taken for any instances of intimidation and/or harassment.

8. Principles for acceptable use of the Internet

8.1 All Staff and Students

The following are acceptable uses of the internet for staff and students:

- The use of email for communication: between colleagues, between student(s) and teacher(s), between student(s) and student(s), between staff and vendors/other professionals.
- Use of the Internet to investigate and research school subjects, cross-curricular themes or topics related to social and personal development.
- The development of pupils' competence in ICT skills and their general research skills.

Online and other activities which are **not permitted** include:

- Searching, viewing or retrieving materials that are not related to the aims of the curriculum.
- Copying, saving or redistributing copyright-protected material, without approval.
- Subscribing to any services or ordering goods or services, unless specifically approved by the School.
- Playing computer games or using other interactive 'chat' or 'social' sites unless specifically approved by the School.
- Using the network in such a way that use of the network 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 a user (such as: home address, email address, phone number, etc).
- Downloading software.
- Taking and storing images of students (see the Schools Photograph, Video and CCTV policy).
- Any activity that violates a school rule.



8.2 Staff

Staff are only permitted to use the Internet for personal use (this includes email) during student non-contact time.

9. Responsibilities

9.1 The School

The School will follow the guidelines as outlined in "Keeping children safe 2022"

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1080047/KCSIE_2022_revised.pdf

- Use a firewall to filter and monitor access.
- Ensure virus and anti-malware protection is installed and updated regularly.
- Regularly discuss acceptable use with children and remind them of the school's policy and rules.
- Ensure teachers guide students toward appropriate materials on the Internet.
- Appoint a member of SMT with responsibility for Child Protection and Safeguarding.
- Ensure only those people with authorised access can access the School's IT network.

9.2 Students

Students will:

- Have equal access to school-controlled email in a safe and secure environment.
- Be taught all the skills in order to use Internet and email as an ICT tool.
- Know how to report any concerns they may have.
- Use Internet and email to support, enhance and develop all aspects of the curriculum.
- Be given the chance to develop Internet and email skills.

9.3 Staff

Staff will:

- Ensure they keep data safe and secure.
- Conduct themselves professionally online; they must not allow students access to their own data through social networking sites such as Facebook; staff members are advised to block children from their class and school.
- Inform Mrs Yar or Mrs Lee-Douglas of any issues or concern.

9.4 Parents

Parents will:

- Conduct themselves in an appropriate manner when contacting staff.
- Parents should raise issues or concerns to the student's mentor as first point of contact.



10. Useful Websites

- www.teachernet.gov.uk
- www.thinkuknow.co.uk/teachers
- www.childnet.com
- www.kidsmart.org.uk
- www.ceop.gov.uk/reportabuse/index.asp
- www.everychildmatters.gov.uk
- www.nen.gov.uk/hot_topic
- [National Online Safety | Keeping Children Safe Online in Education](#)



Appendix 1 – Summary of Rules

CA London understands the importance and benefits of using technology; however, also recognises that safeguards need to be in place. This ensures students at the School, as well as the School's data, are kept safe at all times. All staff and students must agree to the following rules:

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc. for School purposes.
- I will not download or install software on School equipment.
- I will only log on to the School network and systems with my own user name and password.
- I will follow the School's ICT security system and not reveal my passwords to anyone and change them if asked.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal (if a student accidentally comes across any such material they should report it).
- **Images of students and staff will only be taken, stored and used for school purposes in line with the School's Photography, Video and CCTV policy and will not be distributed outside the School network without the permission from the Head of School.**
- I will ensure that my online activity, both in School and outside School, will not cause distress to staff, students or others.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community
- I will respect the privacy and ownership of others' work online at all times.
- I will **NOT** attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged.
- I understand that these rules are designed to keep students safe and that if they are not followed, School sanctions will be applied.
- I understand that I am liable for replacement costs if computer equipment is used inappropriately and without due care.

In addition, students must agree to these additional rules:

- I will only use my School email address.
- I will not give out any personal information such as name, phone number or address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher.



Appendix 2.1 – Student Signature Sheet

Student Name:

Laptop Number:

Email address:

@centreacademy.co.uk

Please could parents/carers read and discuss this policy with their child and then sign and return to Mrs Yar.

- I agree to comply with the terms of this policy and understand that if I do not then my email account and/or network access will be withdrawn. I understand that I will also be subject to disciplinary procedures.

Student Signature:

Parent/Carer Signature:

Date:



Appendix 2.2 – Staff/Visitor Signature Sheet

Please read, sign and return to the School Office.

- I have read and agree to comply by the terms of this Policy.

Name:
(please print)

Signature:

Date:
