North London Collegiate School Dubai

POL/SF005 NLCS Dubai Safer Use of Technology Policy – Whole School

Policy Title:	NLCS Dubai Safer Use of Technology Policy – Whole School
Policy Number:	POL/SF005
Version:	Version 3
Effective Date:	January 2024
Scheduled Review Date:	January 2028
Supersedes:	Version 2 – Implemented March 2019
Approved By:	Deputy Head of Junior School

1. Scope

This policy is addressed to all students, and parents are encouraged to read it with their child. A copy of the policy is available to parents on the NLCS Website, Parents, School policies, and the School actively promotes the participation of parents to help the School safeguard the welfare of students and promote e-safety. This policy takes into account:

- Keeping Children Safe in Education - DFE (2023)
- Education for A Connected World – UKCIS (2020)

and is based on UK best practice and UAE National Law.

This policy applies to the Whole School and should be read in conjunction with the following policies:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-bullying Policy

This policy relates to e-safety and the acceptable use of technology, including and not exclusive too:

- The world wide web
- Communication – email, social media, instant messaging, video calls
-

- Devices – phones, smart watches, laptops, e-readers, tablets, computers, camera. storage
- Applications and websites
- Virtual learning environments e.g Teams
- Cameras and other devices with the capability for recording and/or storing still or moving images
- Social networking, micro blogging and other interactive web sites
- SMART or interactive boards

It applies to the use of any of the above on School premises and also any use, whether on or off School premises, which affects the welfare of other students, or where the culture or reputation of the School are put at risk.

Staff are subject to a separate policy which forms part of their contract of employment.

2. Aims

The aims of this policy are:

- to encourage students to make safe, secure, appropriate and effective use of technology
- to safeguard and promote the welfare of students, in particular by anticipating and preventing the risks arising from:

(a) Content - exposure to inappropriate material (such as pornographic, racist, extremist or offensive materials).
(b) Conduct - the sharing of personal data, including images, cyberbullying and other forms of abuse.
(c) Contact - inappropriate online contact to or from others.

- to minimise the risk of harm to the assets and reputation of the School.
- to help students take responsibility for their own e-safety (i.e., limiting the risks that children and young people are exposed to when using IT).
- to ensure that students use IT safely and securely and are aware of both external and peer- to-peer risks when using IT.

3. Roles and Responsibilities

The Governing Body

- The Governing Body has overall responsibility for the safeguarding procedures within the School, the day-to-day responsibilities for which are delegated to the Principal.
- The Nominated Safeguarding Governor takes leadership of the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Governing Body.
- The Governing Body will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of how students may be taught about safeguarding, including online safety, through the School's curricular provision, ensuring relevance, breadth and progression.

- The Governing Body will undertake annual training on online safety in order to ensure best practice is followed.

Principal

- Promote and foster a culture of safeguarding with a clear focus on online safety and e-safety.
- Delegation of day-to-day responsibility for the online safety of students to the Designated Safeguarding Leads.
- Ensure that policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance.
- Ensure the School implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures.

Designated Safeguarding Leads (DSLs)

- Responsible for managing online safety incidents in the same way as other safeguarding matters in accordance with the School's Safeguarding and Child Protection Policy.
- Ensure regular and frequent training is undertaken by all staff.
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life for students and parents.
- Liaise with an IT Team monitoring the School's IT safety practices and the implementation of the procedures, to assess whether any improvements can be made to ensure the online safety and wellbeing of students.
- Update the Senior Team regularly by the Designated Safeguarding Leads on the operation of the School's safeguarding arrangements, including online safety practices.

IT Manager

The IT Manager together with their team, is responsible for the operation of the School's filtering system to ensure that students are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

The IT Manager is responsible for ensuring:

- that the School’s technical infrastructure is secure and is not open to misuse or malicious attack;
- that users may only access the School’s networks and devices if properly authenticated and authorised;
- establishing appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online.
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- that logs of student network access are extracted, inspected and saved on a regular basis.

- Student and Staff login credentials on all school systems are updated periodically and password changes enforced.

All staff

- act as good role models in their use of technology, the internet and mobile electronic devices.
- are expected to comply with the separate policies that form part of their contract of employment and have knowledge and understanding of this policy.
- must report any inappropriate materials/sites they or their students have been able to access to the DSL and IT Team so that these sites can be added to the firewall filtering process.
- Ensure that any incidents of cyber-bullying are reported and dealt with appropriately in line with the School Behaviour Policy.
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.

Parents

The role of parents in ensuring that students understand how to stay safe online is crucial. The School expects parents to promote e-safety and to:

- support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures.
- talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour.
- encourage their child to speak to someone if they are being bullied or need support.
- If parents have any concerns or require any information about e-safety, they should contact the Designated Safeguarding Leads.

4. E-Safety

The School provides internet access, an e-mail system and online educational platforms to students to support their academic activities and to maximise the educational opportunities presented by such access.
Students may only access the School's network when given specific permission to do so. All students will receive guidance on the use of the School's internet and e-mail systems (Appendix 1) and use of mobile phones (Appendix 2).
The School has a monitoring system, by which any misuse or attempted misuse of the School's network and devices can be identified in real time and reported to the appropriate person for investigation. In the meantime, the School will conduct periodic spot checks to identify any misuse of the School's network.

For the protection of all students, their use of e-mail and of the internet will be monitored by the School. Students should remember that even when an e-mail or something that has been downloaded has been deleted, it can still be traced on the system. Students should not assume that files stored on servers or storage media are always private.

If a student is unsure about whether he/she is doing the right thing, he/she must seek assistance from a member of staff.

5. Education and Training

The School's curriculum includes information about e-safety to build resilience in students to protect themselves and their peers. E-safety means limiting the risks that children and young people are exposed to when using technology, so that all technologies are used safely and securely.
Students are taught about general e-safety within Personal Social Health Education, Moral Education, small group work and/or computing lessons where relevant. These sessions offer guidance on aspects, such as the safe use of social networking sites and cyberbullying, blocking, removing contacts from lists, sharing of personal data and saving evidence where bullying has taken place.

Other example areas which students are educated on are:

- the risks associated with using the internet and how to protect themselves and their peers from potential risks;
- to be critically aware of content they access online and are guided to validate accuracy of information;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour;
- how to report cyberbullying and / or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly.

The School provides e-safety training to staff to protect students and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements.
Parents are encouraged to attend e-safety talks held at the School. All parents and staff also have access to the National Online Safety resources and training courses.

6. Procedures

- Students are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and legal.
- If a student is aware of misuse by other students, he/she should talk to a teacher about it as soon as possible.
- If a student is worried about something that he/she has seen on the internet, he/she should talk to a teacher about it as soon as possible.
- Any misuse of the internet will be dealt with under the School's Behaviour Policy as highlighted below, in section 7.

6.1 Cyber-bullying

- Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.
- Students must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-Bullying Policy.
- If a student thinks that he/she has been bullied or that another person is being bullied, he/she should talk to a teacher about it as soon as possible. Students should remember the following:

    - Always respect others - be careful what you say online and what images you send
    - Think before you send - whatever you send can be made public very quickly and could stay online forever
    - Do not retaliate or reply online
    - Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this.
- If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures as set out in the School's Safeguarding and Child Protection Policy.

6.2 Photographs

- Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- Students may only use cameras or any mobile electronic device with the capability for recording and/or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image. Students should be reminded of the laws in the UAE regarding photographing others without consent.
- In the event that a reasonable suspicion exists that inappropriate material is stored on a device, a member of staff will place the device in safe keeping and contact the parents to seek permission to access the images.
- The posting of images, which in the reasonable opinion of the Vice Principal (Pastoral Care) and the Head of the Junior School, is considered to be offensive on any form of social media or websites such as YouTube etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material,irrespective of whether the image was posted using School or personal facilities.
- Students are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the School and is a criminal offence in the UAE. The School will treat incidences of sexting (both sending and receiving) as a safeguarding matter under the School's child protection procedures. Students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

7. Sanctions

- Where a student breaches any of the School rules, practices or procedures set out in this policy or the appendices, sanctions that are appropriate and proportionate to the breach will be applied, including, in the most serious cases, expulsion.
- Other sanctions might include increased monitoring procedures or withdrawal of the right to access to the School's internet and e-mail facilities. Any action taken will depend on the seriousness of the offence.
- Unacceptable use of electronic equipment or the discovery of inappropriate data or files could lead to the device being placed in the Safeguarding safe for safe keeping, or deletion of the material in accordance with the practices and procedures in this policy and the School's Behaviour Policy. Parents will be informed of any action taken.
- Where there is concern that a student maybe accessing inappropriate material or conducting other prohibited activities detailed within this document, the School maintains the right to monitor a student's activity in real time. This action may only be sanctioned by a Vice Principal and in conjunction with Safeguarding leads.
- The School reserves the right to charge a student or his/her parents for any costs incurred to the School, or to indemnify any significant liability incurred by the School, as a result of a breach of this policy.

8. Communication Between Students and Staff

- Students must use their School email accounts for any email communication with staff. Communication either from a student's personal email account or to a member of staff's personal email account is not permitted.
- Students should avoid using mobile phones to speak to or send messages to staff whilst in or out of School. Telephone numbers should not be exchanged, displayed or stored. Any messages or phone calls that are sent for urgent reasons should be brief and courteous.
- Students must not access or use social networking sites of members of staff and no student or staff should be friends on social media.
- The leader of an educational visit will carry a mobile phone supplied by the School and, as part of the preparations for the visit, will ensure that relevant numbers are exchanged with students and other adults taking part in the visit.
- Students taking part in such visits should avoid using mobile phones to speak to or send messages to staff except in emergencies. Any messages that are sent should be brief and courteous.
- Inappropriate communications - If there are reasonable grounds to believe that inappropriate communications have taken place, the School will require the relevant mobile phones to be produced for examination. The usual disciplinary procedures will apply. Students may expect to have mobile phones placed in safe keeping if there has been a breach of these rules.

9. The Liability of the School

- Unless negligent under the terms of this policy, the School accepts no responsibility to the student or parents caused by or arising out of a student's use of the internet, e-mail or any electronic device whilst at School.
- The School does not undertake to provide continuous internet access. E-mail and website addresses at the School may change from time to time.

10. Monitoring and Review

- The School reserves the right to monitor the use of the internet and email.
- All serious e-safety incidents should be reported to the Vice Principal (Pastoral Care) or the Head of the Junior School and will be recorded on the student's file, on CPOMS.
- The Vice Principal (Pastoral Care) and the Head of the Junior School are responsible for the implementation and review of this policy and will consider the record of e-safety incidents and new technologies where appropriate, to consider whether existing security and e-safety practices and procedures are adequate.
- Consideration of the efficiency of the School's e-safety procedures will be included in the Governors' annual review of safeguarding.

APPENDIX 1

Internet Use and E-mail Protocol

Introduction

We want each student to enjoy using the internet, and to become proficient in drawing upon it both during their time at School, and as a foundation for their further education and career. However, there are some potential drawbacks with e-mail and the internet, both for students and for the School.
The purpose of these rules are to set out the principles which students must bear in mind at all times and also the rules which must be followed in order for all students to use the internet safely and securely.
The principles and rules set out below apply to all use of the internet, including social media, and to the use of e-mail in as much as they are relevant. Failure to follow these rules will constitute a breach of discipline and will be dealt with in accordance with the School's Behaviour Policy.

Access and security

Computer facilities are provided within the school to allow students to extend their IT skills and to use as a tool in all curriculum subjects to research, analyse, exchange and present information. Priority is always given to educational activities over private use.
Students are given their own user ID and are responsible for work carried out under their own name. Passwords protect the School's network and computer system. Students should set their own password and should not use obvious passwords such as their family name or birthdays etc. Passwords should not be divulged to anyone. If a student believes that someone knows their password, they must change it immediately.
If there is a problem with passwords, students must approach the IT department, in person, for assistance. The IT department will verify the student's identity by checking the student's photograph on the School Information Management System database before resetting a student's password.
Students must log off or lock their workstations if they leave the workstations for any period of time.
Students must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.

The School has a Firewall in place to ensure the safety and security of the School's networks. Students must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the firewall must be reported to the Form/Class Tutor or the IT Department.
The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of students.

Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to e-mails. If a student thinks or suspects that an attachment, or other material to download, might contain a virus, he/she must speak to their class teacher and/or the IT department before opening the attachment or downloading the material. Students must not disable or uninstall any anti-virus software on the School's computers.

Use of the internet

Students are permitted to use the School's computer systems for personal or leisure use, however, priority must always be given to someone with school work to do.

Students must take care to protect personal and confidential information about themselves and others when using the internet, even if information is received or obtained inadvertently.
Students should not put personal information about themselves, for example their full name, address, date of birth or mobile number, online. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.
Students should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - students must not copy (plagiarise) another's work.

Students must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, any form of bullying, pornographic, defamatory or criminal activity. Use of IT in this way is a serious breach of discipline. Students must tell a member of staff immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

Students should not enter into any contractual commitment using the internet when in the care of the School, or otherwise associated with the School, whether for themselves or on behalf of another (including the School).
Students must not bring the School into disrepute through their use of the internet.

Use of e-mail

E-mail should be treated in the same way as any other form of written communication. Students should not include or ask to receive anything in an e-mail which is not appropriate to be published generally, or which the student believes the Vice Principal (Pastoral) or the Head of the Junior School, and/or his/her parents would consider to be inappropriate.

Students must not send, search for or (as far as students are able) receive any e-mail message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of a terrorist related nature, sexist, any form of bullying, religious extremism, pornographic, defamatory or criminal activity. If students are unsure about the content of a message, they must speak to a member of staff. If a student comes across such material, he/she must inform a member of staff as soon as possible. Use of the e-mail system in this way is a serious breach of discipline. The School will take no responsibility for any offence caused by a student as a result of downloading, viewing or forwarding inappropriate e-mails.

Students' School e-mail accounts can be accessed from home via Office365. The School will not forward e-mails received during the School holidays.
Trivial messages and jokes should not be sent or forwarded through the School's e-mail system. Not only could these cause distress to recipients (if inappropriate) but could also cause the School's IT system to suffer delays and/or damage.

All correspondence from your School e-mail account must contain the School's disclaimer.
Students must not read anyone else's e-mails without their consent.

APPENDIX 2

Student mobile electronic devices

Use of mobile electronic devices

"Mobile electronic device" includes, without limitation, mobile phones, smartphones/watches, tablets and laptops.

Mobile electronic devices must be placed on silent and kept in bags or lockers during registration, lessons and extra-curricular activities.

In emergencies, students may request to use the School telephone. Parents wishing to contact their children in an emergency may telephone the School Reception and a message will be relayed promptly.

Students may not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Principal in writing.

Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline, whether or not the student is in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's Anti-Bullying Policy and Behaviour Policy).

The School reserves the right to place a student's mobile electronic device in safekeeping for a specified period of time, if the student is found to be in breach of these rules. Students' parents will immediately be notified if this happens. The student may also be requested to not bring a mobile electronic device into the School temporarily or permanently and at the sole discretion of the Senior Team and Designated Safeguarding Leads.

The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises.

Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see the School's Behavior Policy on the searching of electronic devices.

APPENDIX 3

Senior School Student Policy on the Safer Use of Technology and E-Safety

Using the School's IT Facilities:

- I will use the School computer network and facilities in a responsible and careful manner.
- I will only access the School computer network using my own username and password, and will keep my log in details private
- I will only open emails, attachments and links received from an approved/reliable source
- I will not view, download or share unsuitable or offensive material and will immediately inform a member of staff if I accidentally do so.
- I will not attempt to bypass the School's internet filtering system.
- I understand that the School monitors the use of emails and internet.
- I will not use the School's system to order goods or services online.
- I will not use the School's system to do anything online which may legally bind myself or the School.

Responsible Behaviour:

- I will not cyberbully fellow students, staff or others.
- I will give priority to fellow students who wish to use the facilities to complete schoolwork.
- I will not copy (plagiarise) material on the internet.
- I will only take photographs and video recordings, and post these online, with the permission of those appearing in the photograph/recording.
- I will not bring the School into disrepute through my use of the internet.
- I will not use my personal email account to contact a member of staff.
- I will not contact members of staff via their personal mobile phones, personal email accounts, social networking sites etc.

Using Your Own Device in School:

- I understand that the use of my own mobile electronic device in School is a privilege and dependent on me using the device safely and responsibly.
- I understand that the use of my device in School is entirely at my own risk and I must ensure that my device is not damaged, lost or stolen.
- I understand that my device must be placed on "silent" and kept in my bag/locker during registration, classes and extra-curricular activities.
- I will ensure my device is password protected and has up to date antivirus software

Online Safety:

- I will not post my personal information such as my home address, email address, telephone number etc. online.
- I will not post personal details of my fellow students, staff or others online
- I will ensure my privacy settings are set correctly on social networks.
- I will not reply to offensive messages and will block or report the sender.

I confirm I have read through the above rules with my child and that he/she understands these rules and agrees to abide by them.

Student's Signature: _____

Student's Name: _____

Date: _____

Parent's Signature: _____

Parent's Name: _____

Date: _____

APPENDIX 4

Lower School Student Policy on the Safer Use of Technology

These rules will keep me safe and help me to be fair to others when using technology at school.

Using the School's IT Facilities:

- I will only use the School's technology for schoolwork and homework.
- I will take care when handling the School's technology equipment, including mobile devices (e.g. iPads, iPods etc.)
- I will not bring files into School without permission or upload inappropriate material to my workspace.

Responsible Behaviour:

- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my passwords secret from other students.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will only visit Internet sites that are appropriate for School.
- The messages I send, or information I upload, will always be polite and sensible.
- I will respect copyright rules and give credit to work that is not my own.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not take a photograph, record video or audio of anyone without receiving their permission first.

Using your own device in School:

- Any personal mobile devices will remain in a locker and not be used during the School day.
- I understand that having personal devices in School is at my own risk.

Online Safety:

I will not give my home address, telephone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.

- I will only e-mail people I know, or a responsible adult has approved.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher/responsible adult.

I confirm I have read through the above rules with my child and that he/she understands these rules and agrees to abide by them.

Student's Signature: _____

Student's Name: _____

Date: _____

Parent's Signature: _____

Parent's Name: _____

Date: _____