E-SAFETY POLICY

The NCS aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Sixth Form community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams. If you feel your students or staff are at risk, please report it to the Anti-Phishing Working Group

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (2023) and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all students in all situations, and a more personalised or contextualised approach may often be more suitable.

Senior Leadership Team

- To ensure that there are appropriate and up-to-date policies regarding online safety; including an acceptable use policy, which covers acceptable use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- To ensure that online safety is embedded within the curriculum, which enables all students to develop an age-appropriate understanding of online safety.
- To support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- To ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- To ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- To audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL)

Details of the school's DSL (and deputies) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

- The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the sixth form
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the NCS child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the sixth form behaviour policy
- Updating and delivering staff training on online safety

- Liaising with other agencies and/or external services if necessary

Managed device/IT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at the sixth form, including terrorist and extremist material
- Ensuring that the sixth form's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a continual and ongoing basis.
- Blocking access to potentially dangerous sites and preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Security strategies will be discussed with the IT provider.

All student iPads are managed via Apple School Manager and Meraki, which allows for control and lockdown of settings, such as preventing the install and removal of Apps and using unauthorised accounts.

Lightspeed relay is used to filter all web traffic on and offsite on any internet connection. If a student or staff member would like a new app or site added to the allowed this, this is first checked by the DSL/SLT.

All staff and volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the sixth form's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the sixth form behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the sixth form's ICT systems and internet

Teaching and Learning

- The purpose of Internet use in Newham Collegiate Sixth Form (the 'NCS') is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the management information and business administration systems.
- The Internet is an essential element in 21st century life for education, business and social interaction. The NCS has a duty to provide students with quality Internet access as part of their learning experience.
- Students use the Internet widely outside the Sixth Form and will need to learn how to evaluate Internet information and to take care of their own safety and security.
- During any lockdown, students will be able to access all lessons remotely and safeguards have been put in place to ensure synchronous learning is safe for students and teachers.

Benefits of using the Internet in Education Include

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between Students world-wide through video-conferencing;
- Access to experts in many fields for students and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the DfE and other educational agencies;
- Access to learning wherever and whenever convenient.

Use of Mail

- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Excessive social e-mail use can interfere with learning and will be restricted.
- The forwarding of chain letters is not permitted.
- Under no circumstances should staff contact students, parents/carers or conduct any school business using personal e-mail addresses.
- NCS e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) but not for contact with parents/students.

Published Content - Website

- The contact details on the Website should be the Sixth Form address, e-mail and telephone number. Staff or Students' personal information will not be published.
- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents or carers will be obtained before photographs of Students are published on the Sixth Form Web site.
- Students' work can only be published with the permission of the Student.

Educating students about online safety

We will establish and embed an online safety curriculum to raise awareness and promote safe and responsible Internet use amongst students by:

- Ensuring education regarding safe and responsible use precedes Internet access;
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE);
- Reinforcing online safety messages whenever technology or the Internet is in use;
- Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide Students in on-line activities that will support the learning outcomes planned for the Students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Social Networking and Personal Publishing

- Students are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, Sixth Form, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Students are advised not to place personal photos on any social network space. They consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location (e.g. house number, street name, academy, shopping centre).
- Teachers must not run social network spaces for students on a personal basis or to give/accept friendship requests from students on social networking sites.
- The Sixth Form is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- The Sixth Form will work in partnership with parents, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Staff must refuse an invitation to link with a colleague on a social networking site until they have checked with the colleague that the request is genuine.

Educating parents about online safety

The sixth form will raise parents' awareness of internet safety in letters, safeguarding bulletins or other communications home, and in information via our website.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school, through the pastoral programme, will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups.

The sixth form will use the safeguarding bulletin to address online safety, including cyberbullying so that parents are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the sixth form will follow the processes set out in the behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the sixth form will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

The Sixth Form's staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the sixth form rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the sixth form complaints procedure.

Acceptable use of the internet in the Sixth Form: students and staff

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

All staff will be informed about the Sixth Form e-Safety Policy and its importance explained

Use of the sixth form's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff should not keep photos or videos of Students on their personal electronic devices.

We will monitor the websites visited by students, staff, volunteers, governors to ensure they comply with the above.

Students using mobile devices in the Sixth Form

Students may bring mobile devices into the sixth form, but are not permitted to use them during:

- Lessons
- Tutor time
- Clubs before or after school, or any other activities organised by the sixth form
- Corridors

Any use of mobile devices in the sixth form by students must be in line with the acceptable use agreement and with the permission of the teacher.

Mobile devices can only be used in private study/canteen, where students may listen to music whilst studying. The sending of abusive or inappropriate text messages is forbidden.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the sixth form behaviour policy, which may result in the confiscation of their device.

How the sixth form will respond to issues of misuse

Where a student misuses the sixth form's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use . The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the sixth form's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The sixth form will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, on online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, bulletins and staff meetings).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL (and deputies) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on online safeguarding issues as part of their safeguarding training.

Monitoring arrangements

The Principal/ DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Mouhssin Ismail, Principal. At every review, the policy will be shared with the governing board.

Links with other policies

This E- safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices

- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: NCS Acceptable use agreement

Newham Collegiate
Sixth Form Centre

A specialist centre for Science and Mathematics

Acceptable Use Agreement for Students **Section 1: ICT Agreement**

1. I will only log onto the NCS I pad with my own username and password
2. I will not reveal my password(s) to anyone
3. I understand that my use of the Internet and other IT can be monitored, and that my teachers and other school staff will sometimes look at how I am using IT and what I am storing on my devices and other school devices
4. I understand that my teachers will look at and assess my work that I keep in my files
5. I understand that when I use IT, this is logged on school systems and that my teachers can see this
6. I understand that if I do something that I should not when using IT; for example, look at sites I am not supposed to, download Apps that I should not, or use offensive language or images; that school staff will respond to this. This may involve a sanction, informing my parents, my carers, and when it is really serious, the police and other people external to the school, such as social workers
7. I will make sure that all IT communications with other students, peers, teachers or others is responsible, sensible and appropriate and, most importantly, that it is not offensive or upsetting in any way
10. I will be responsible for my behaviour when using the Internet
11. I will not give out any personal information such as name, phone number or address; this includes the details of other students or adults to anyone
12. I will not share photos/images/videos of myself or anyone else that are inappropriate with anyone and will inform a member of staff if anyone sends something like this to me
13. I will respect the privacy and ownership of others' work online at all times
15. I understand that if I bring unauthorised electronic equipment into school and use it, that it will be confiscated and my parents/carers will be asked to come into school to collect it
16. I will report any concerns that I have about myself or anyone else online to a member of staff

Section 2: I pad agreement

1. I understand that the NCS has provided me with my iPad to aid my learning
2. I understand that the NCS has invested a significant amount of money in the device, so I will look

after the device
4. I will delete any personal downloads if the space is needed for learning resources
5. I will only take/use photos, images and videos of pupils and/or staff with their permission. I understand that I should not take pictures or videos of other students and staff without their permission
6. I will ensure that all my online activity, both in school and outside school, will not cause anyone, (my family, the NCS, the staff, students or others) distress, upset or bring them into disrepute

10. I understand that the reason I have been given a device is for learning and making progress, my apps and the content of my device should show this. I will not download any apps not relevant to aiding my learning
11. I will keep my device within the supplied screen protective cover at all times

12. I will not try to get around security or web filtering on any device I use at school
13. I understand that connecting my mobile device to a mobile hotspot is unacceptable in school.
14. I will only use the genuine device charger provided to me by the NCS
15. I will use my device when appropriate, ensuring that the apps I use are for learning purposes
16. I will not message others during lesson time
17. I understand that any web activity on my iPad is monitored by the IT staff and safeguarding team at the NCS; for example, looking at/ accessing a website I am not supposed to on my iPad or if a particular search term is used such that might be offensive/ involve swearing, violence, gambling and sexual content at any time

I understand that these rules are designed to keep me safe.

Newham Collegiate
Sixth Form Centre

A specialist centre for Science and Mathematics

Acceptable Use Agreement for Students

I have read this document and agree to follow the rules in this document and to support the safe and responsible use of IT at the NCS:

- • I understand that I have been supplied this device for the sole use of supporting my learning and that I am responsible for this device during my time at the NCS
- • I understand that the device remains the property of the NCS, should I leave the NCS before completing all exams that the device will have to be returned in good condition, should this not happen the NCS reserves the right to charge for repair or replacement of the device
- • I understand that should the device be accidentally or maliciously damaged, vandalised, lost or stolen that the school reserves the right to charge to repair or replacement of the device
- • I understand that I must replace or pay for the charging cable and adapter if lost or damaged
- • I understand that these rules are designed to keep students safe and that if they are not

  Followed, school sanctions will be applied. The NCS has a duty and the right to report any illegal or significantly inappropriate to the police or other agencies for further action
  Any breach of the I pad agreement the school will follow the procedures set out in the behaviour/exclusion policy and take appropriate actions

.