Title:	Online safety and Acceptable Use Policy
Associated Policies:	• Safeguarding and Child Protection • Data Protection • Freedom of Information • Anti-Bullying • Peer on Peer Abuse

1	Policy Statement
	1.2 Northampton School for Girls acknowledges that Information Technology (IT) is an integral and critical resource for students, staff, governors, volunteers and visitors through the delivery and support of teaching and learning and supporting pastoral and administrative functions of the Academy however, the IT resources and facilities our academies use also pose risks to data protection, online safety and safeguarding. Northampton School for Girls is committed to promote the welfare and safety of our students when using digital technologies. The aim of this policy is to outline the acceptable and safe use of digital technology for all stakeholders and how through thus use they are safeguarded
2	Who does this policy apply to?
	2.1 This policy applies to all 'users' of Northampton School for Girls information and relates to use of all IT facilities and services provided by the school (see paragraph 4 for definitions). **2.2** This policy applies not only to use of Northampton School for Girls digital technology equipment in school but also applies to the use of school systems and equipment off school premises and the use of any personal devices or equipment on or off school premises. **2.3** All users will sign the relevant Acceptable Use Policy documents (Appendices A-)
3	Who is responsible for carrying out this policy
	3.1 The implementation of this policy will be monitored by the Senior Leadership Team and the governors of Northampton School for Girls
4	What are the principles behind this policy?
	4.1 The aim of this policy is to: • Set guidelines and rules on the use of school IT resources for staff, students, parents/carers and governors. • Establish clear expectations for the way all members of the academy communities engage with each other online. • Support the school's policies on data protection, online safety and safeguarding providing a clear understanding of everyone's online safety requirement. • Prevent disruption to the academy through the misuse, or attempted misuse, of IT systems. • Support the school in teaching students safe and effective internet and IT use. • Promote safe working practices for staff and students for remote learning during the COVID19 global pandemic. **4.2** Northampton School for Girls provides information systems for the use of all staff, students, governors and volunteers on the understanding that: The user has read and agreed to abide by this policy. • The user does not misrepresent him/herself or attempt to impersonate any other person or entity whilst using school IT systems. • The user does not publish libelous material using the school IT systems e.g. via blogs or online journals or videos published on social media.

- Northampton School for Girls reserves the right to suspend access, retain equipment loaned to staff or students and view any data held on its systems whilst investigating a breach of this policy or whilst investigating any other matter in which NSG has a legitimate interest.

Northampton School for Girls has the right to monitor the use of all devices including mobile devices issued, for internet use, e-mails and all aspects of the network/computer system. Further detail is included within paragraph 5.9 of this policy.

4.3 Any student, staff member, governor, volunteer or visitor who are in breach of this policy and engage in any of the unacceptable activity covered under the policy may face disciplinary action in line with the school's respective disciplinary policies. Depending on the nature of the breach, other sanctions such as revoking permission to use the Trust's IT systems, may be considered where appropriate.

4.4 This policy has been developed to comply with:

Data Protection Act 2018,
The General Data Protection Regulation,
Computer Misuse Act 1990,
Human Rights Act 1998,
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,
Education Act 2011,
Freedom of Information Act 2000,
The Education and Inspections Act 2006, Keeping Children Safe in Education 2021,
Searching, screening and confiscation: advice for schools

5 Procedures

Access

5.1 Access to Northampton School for Girls information systems and user accounts is obtained via a unique username and password. This is provided to the user by the IT Support team on the understanding that:

- Any password issued to a user becomes his/her responsibility. No password should be shared with other users or third parties.
- Sharing a password may result in suspension of the user's account.
- Using the account of another user will result in immediate suspension of access to the school's systems and referral to the Senior Leadership Team for consideration under Northampton School for Girls disciplinary procedures.
- The only software authorised for use on Northampton School for Girls information systems are those programs already installed on the machinery by the IT Support team or authorised for use in school activities. This includes online services. Any attempt to introduce or install software onto the school systems will be viewed as an intention to damage Northampton School for Girls property and could constitute a breach of safeguarding and/or data protection regulations, resulting in disciplinary action.
- Any user who causes damage, directly or indirectly, to any equipment may be refused the right to further use of the equipment and billed for its repair or replacement.
- Gaining, or any attempts to gain, access to restricted areas of the network, or to any password protected information, without approval from authorised personnel will be considered unacceptable use and a breach of this policy.

5.2 Other examples of unacceptable use following access to a school's information system include (but is not limited to):

- Using the school's IT facilities and services to breach intellectual property rights or copyright.
- Using the school's IT facilities and services to bully or harass someone else, or to promote unlawful discrimination.
- Activity which defames or disparages the school, or risks bringing the school into disrepute. This includes canvassing, lobbying, advocacy, or personal endorsement that has not been ratified by the Trust.
- Sharing confidential information about the school, its pupils, or other members of the school community.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Removing, deleting or disposing of IT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Promoting a private business, unless that business is directly related to the school.

Storage

5.3 All users are provided with storage space for their files on the school's servers referred to as their "user area". This storage is provided on the understanding that:

- All data is stored in the approved area (Google Drive). Any data saved in areas other than approved locations may not be backed up by the IT team.
- No inappropriate material is stored e.g. pornography or libelous material.
- No material is stored that infringes copyright i.e. illegal copies of any audio or video file or software program.
- No personal information about others is stored without direct reference to the Data Protection Act.
- Northampton School for Girls reserves the right to withdraw access to files and materials whose ownership is in question whilst an investigation is carried out.
- Users may not use the school's IT facilities or services to store personal non-work-related information or materials (such as music, videos, or photos). Use of the school's IT facilities or services for personal use may put personal communications within the scope of the school's IT monitoring activities (see paragraph 1.4). Where breaches of this policy are found, disciplinary action may be taken.

Internet

5.4 Northampton School for Girls provides access to the internet in as unrestricted a manner as possible on the understanding that:

- No user will access, download, store, bookmark or record websites containing inappropriate content.
- No user will access websites containing online games or instant messaging services unless it has been an identified learning function which has been agreed by the Head Teacher.
- No user will attempt to access online shops or services whose age requirements they do not meet e.g. eBay or any other websites which are not relevant for work purposes.
- Northampton School for Girls reserves the right to filter or restrict access to certain internet sites. Any attempts to bypass the school's filtering mechanisms will be considered unacceptable use of the school's IT systems.
- Staff will adhere to the school's expected professional conduct with particular regard to use of social media and use of email to protect themselves online and avoid compromising their professional integrity.

Email

5.5 Electronic mail accounts are provided for everyone at Northampton School for Girls on the understanding that:

- Staff will only communicate with students by email using their, and the students' school email address.
- The content of any email sent will be appropriate in terms of its language and subject matter regardless of its destination. Users will take care with the contents of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- The account will be used for work/study purposes only.
- All work/study-related business should be conducted using the email address the school has provided. Staff must not use personal email accounts when communicating with parents/carers and students.

Users will comply with the provisions as set out in the schools' Data Protection Policy particularly in relation to the following:

- when sending sensitive or confidential information by email. For example, any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. Any data breaches will be reported in line with the Data Protection Policy
- raising any concerns to the IT Support team regarding any suspicious hyperlinks in emails or any attachments to emails, unless the source is known and trusted.
- No harmful software will be intentionally transmitted with any message.
- No chain-email messages will be originated by the user or forwarded on from his/her account.
- Northampton School for Girls reserves the right to suspend access to the mail system for any user.
- Northampton School for Girls reserves the right to intercept and monitor any message traffic if it suspects inappropriate content, use of offensive language or malpractice.
- Access to email will terminate when a user leaves Northampton School for Girls.

Social Media

5.6 Northampton School for Girls has official social media page(s), managed by specific appointed members of staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

5.7 Those who are authorised to manage or post to the account must abide by the guidelines as prescribed by the school and by the guidelines of the site.

Data security

5.8 The school takes steps to protect the security of its computing resources, data and user accounts. Further detail of these measures are included within the schools Data Protection Policy. All staff are required to be familiar with and comply with the contents of this policy.

Monitoring of networks and use of IT facilities and services

5.9 Northampton School for Girls have the right to monitor the use of all devices including mobile devices issued, for internet use, e-mails and all aspects of the network/computer system for purposes such as:

Ensuring effective academy and IT operations including:

- resolving a technical issue
- checking for viruses or other network threats
- updating and maintaining devices/software belonging to the school

- checking compliance of devices/software belonging to the school

obtaining information related to academy business;

- investigating unauthorised use where there is a breach with academy policies, procedures or standards;
- prevention or detection of crime; and
- compliance with a Subject Access Request, Freedom of Information Request or any other legal obligation.

5.10 Any staff with concerns about any illegal, inappropriate or harmful material or incident that they become aware of must immediately be reported to their line manager or appropriate person.

Mobile devices provided by Northampton School for Girls

5.11 Any mobile device provided to a member of staff or student by the school is used subject to the following terms as set out in this policy.

5.12 Any damage or faults involving mobile devices provided by the school must be immediately reported to the IT support team.

6 Remote Learning Platform – Google Classroom

6.1 The COVID-19 global pandemic led to schools closing from March-June 2020 and a shift to online learning was needed. After schools opened in June 2020 for some students and September 2020 for all students, a blended, flexible approach is needed so that if students are shielding, isolating or otherwise not attending school can access education. This is clearly set out in DfE guidance.

6.2 Guidance from the DfE https://www.gov.uk/government/publications/remote-educationgoodpractice/remote-education-good-practice states:
The Education Endowment Foundation (EEF) has found that the effectiveness of remote teaching is determined by many of the same factors as determine the effectiveness of live classroom teaching. For example:

- *ensuring pupils receive clear explanations*
- *supporting growth in confidence with new material through scaffolded practice*
- *application of new knowledge or skills*
- *enabling pupils to receive feedback on how to progress*
- Northampton School for Girls believes that reasonable endeavours should be made to ensure that remote learning is as effective as possible, ensuring that students are safe online.

The Head Teacher will ensure that relevant online safety advice for students and parents/carers is available through the school's website/other appropriate means.
The Head Teacher will ensure that students receive appropriate information and guidance about how to access and behave during remote learning sessions.

Northampton School for Girls approves and utilises only Google Classrooms as the learning platform for online learning and provides unrestricted communication to staff classes and student groups on the understanding that:

All users will only use Google Classrooms to teach students and use the wider Goggle package to communicate with colleagues in a school capacity.

- Communication would normally be in the school setting, where this is not possible, communication from home is allowed. In either event it is essential that:

- Staff are appropriately dressed and, in a setting, which allows them to have a professional meeting, including confidential if relevant
- Staff and students do not inappropriately use the chat function (this can be blocked within classes and by admin)
- Only staff may use the video/broadcasting functionality
- It is recommended that students switch off their microphones to limit issues and can use the chat functionality to ask questions. If it is deemed appropriate a student can activate their microphone but should be appropriate.
- There should be no 1-1 teaching. If it if absolutely necessary, prior agreement must be sought from the Head Teacher, you may wish to record these
- Safeguarding and pastoral staff may conduct 1-1 meetings with the permission of the DSL or Headteacher and these again may be recorded unless it compromises the student disclosing.
- Meeting facilitators must ensure that language is professional and appropriate at all times
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- You are mindful of confidentiality if working from home. Ensure that no one else can see the screens when sending information and always lock your laptop when not working, even if it is only for a minute or two. Do not discuss students with anyone other than work colleagues and take care that you cannot be overheard.
- Although online assessment packages such as Hegarty maths, Seneca, SAM Learning, GCSE Pod, etc. can be used it is important that the software is suitably age restricted and that communication within those packages are kept to a minimum. All software used must be agreed to by the Head Teacher (or person with delegated responsibility) and your line manager within school.
- External software must have relevant security measures in place and should for example meet industry standards. Personal information should be limited with these packages, in line with the schools GDPR policy.
- No user will access, download, store, bookmark or record websites containing inappropriate content. It is also important that users do not direct students to websites that contain inappropriate content or have unsuitable age restrictions. Websites such as TikTok, Facebook, etc. are 13+ and YouTube is 13+ and 11+ with parent/carer permission. All video links should be checked for age-appropriateness before distributing to students.
- Staff may record “live” streamed sessions for future use as appropriate within the google classroom. The school deems that by signing the Acceptable Use Policy, consent is given for this.

7 Reporting Online Safeguarding Concerns

We have a responsibility when it comes to online safety and need to ensure the school’s online procedures keep children and young people safe.

The definition of an online safeguarding incident is:

“Any incident that occurs and involves any person (student or adult) where the use of technology (equipment and/or networks) enables or facilitates inappropriate behaviour and harm and/or distress is caused to another person or the reputation of Northampton School for Girls. This may include the use of social media, forums, blogs, open and closed groups, digital images, messages or any other means”.

- The most likely areas of risk to students are:
- Exposure to illegal inappropriate or harmful material
- Subject to harmful online interactions with other users
- The individual’s personal online risky behaviour that then leads to harm

If you think a child is in immediate danger, contact the police on 999. *(Please also refer to the NSG Safeguarding and Child Protection policy)*

If you're worried about a child but they are not in immediate danger, you should share your concerns with the schools Designated Safeguarding Lead and follow the school's child protection procedures reporting this on CPOMS. (*Please also refer to the Anti-Bullying and Peer on Peer policies*)

Please note - Reporting online child abuse images
It's against the law to produce or share images of child abuse, even if the image was self-created. This includes sharing images and videos over social media. If you see a video or image that shows a child being abused: Don't comment, like or share the video or image, as this will distribute it further. Instead Immediately inform the Headteacher or the DSL about when, where and how this has come to your attention.

8 Who is Responsible for Online Safety and what are their safeguarding responsibilities

8.1 Governors
The Safeguarding Governors and the wider governing body must ensure that they have the demonstrable, skills, training and experience to be able to provide appropriate challenge and support to the school management team in regard to monitoring, evaluating and reporting on online effectiveness and safeguarding.

8.2 Headteacher
Headteacher and the Senior Leadership Teams are responsible for determining, evaluating and reviewing online safety and safeguarding practices to encompass teaching and learning, use of school IT equipment and facilities by students, staff and visitors, and agreed criteria for acceptable use by students, school staff and governors of Internet capable equipment for school related purposes or in situations which will impact on the reputation of the school, and/or on school premises.
They will ensure regular assessment of the strengths and weaknesses of practice within the school will help determine inset provision for staff and governors and guidance provided to parents/carers, students and local partnerships.

8.3 Designated Senior Lead (DSL)
The DSL will be responsible for escalating online safety incidents to the relevant external parties e.g. CEOP, local Police, Local Safeguarding Children's Board, social services and parents/carers.
Possible scenarios might include:
- Allegations against members of staff
- Computer crime – hacking of school systems
- Allegations or evidence of 'grooming'
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication

8.4 Online Safety Co-ordinator
- The school has a designated online safety officer who reports to the SLT and co-ordinates online safety provision across the school community.
- The school online safety co-ordinator is responsible for online safety issues on a day to day basis and also liaises with relevant stakeholders including IT support, to ensure the safety of students.
- The online safety co-ordinator maintains a log of submitted online safety reports and incidents.
- The online safety co-ordinator audits and assesses inset requirements for staff, support staff and governor online safety training, and ensures that all staff are aware of their responsibilities and the academy's online safety procedures. The co-ordinator is also the first port of call for staff requiring advice on online safety matters.
- The online safety co-ordinator is responsible for promoting best practice in online safety within the wider school community, including providing and being a source of information for parents/carers and

partner stakeholders. This may include facilitating regular assemblies and other such activities that focus on positive messages and behaviours.

- The online safety co-ordinator will be involved in any risk assessment of new technologies, services or software to analyse any potential risks.

8.5 All staff

- Teaching and support staff are responsible for ensuring that they are aware of the current online safety policy, practices and associated procedures for reporting online safety and safeguarding incidents in line with academy procedures.
- All staff will be provided with an online safety induction as part of the overall staff induction procedures. All staff will attend mandatory online safety training and regular Safeguarding training.
- All staff will ensure that they have read, understood and signed the Acceptable Use Policy relevant to Internet and computer use in school (see Appendix A).
- All teaching staff are to be vigilant in monitoring student Internet and computer usage in line with the policy. This may include the use of personal technology, such as cameras, phones on the school site where there is a cause for concern.
- They are must ensure Internet usage and suggested websites are pre-vetted and documented in lesson planning.
- They must promote and reinforce safe online practices when on and off-site, including providing advice to students on how to report incidents.
- They must report as soon as is practicable any suspected misuse of digitally connected systems to the headteacher or DSL via CPOMS

8.6 IT support staff

Internal IT support staff are responsible for maintaining the academy's networking, IT infrastructure and hardware. IT staff will be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure. IT staff will ensure systems are not open to abuse or unauthorised external access.

IT support staff are responsible for:

- Defending the network and infrastructure of the academy, reviewing activity logs regularly
- Ensuring that users comply with basic access policies and that only trusted devices can connect to the academy network
- Filtering of search facilities is robust and regularly checked for penetration to ensure that the risk of students accessing material that is unsuitable is minimised.
- To keep up to date with current threats and attack trends and take steps to mitigate this and communicate with the management team and Online Safety Co-ordinator.
- To report to the management team and Online Safety Co-ordinator on any network intrusions or other threats to the network
- To ensure that any IT outsourced e.g. connectivity, maintenance, cloud-based services website, email provision, filtering, anti-virus, complies with DfE guidance and Data Protection regulations.
- Promoting basic cyber security practices within the academy e.g. locking computers when away from the desk, using secure passwords, caution when using USB removable drives.
- Ensure external contractors, website designers/hosts will be made fully aware of and agree to the Trust's Online Safety Policy.

9	Definitions
	9.1 IT facilities: includes all facilities, systems and**s** services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the IT service.

	9.2 Users: anyone authorised by the school to use the IT facilities, including governors, staff, pupils, volunteers, contractors and visitors. **9.3 Personal use:** any use or activity not directly related to the users' employment, study or purpose. **9.4 Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the IT facilities. **9.5 Materials:** files and data created using the IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs
10	Policy Review
	This policy will be monitored as part of the Academy's annual internal review and reviewed on a three-year cycle or as required by legislature changes.

Appendix A – Acceptable use of technology policy for staff

I understand that I must use Northampton School for Girls IT facilities in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, other users and students. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

In addition to adhering to the Acceptable Use Policy detailed above and the school's professional codes of conduct, I will comply with the below code of conduct which has been developed to ensure my professional and personal safety when delivering online learning.

For my professional and personal safety:

- I understand and accept that Northampton School for Girls will fully monitor my use of the school digital technology and communications systems.
- I understand that if my activity causes any concerns, safeguarding software installed across the Trust may automatically alert appropriate safeguarding specialists who may choose to investigate depending on the content of the alert.
- I understand that the rules set out in this agreement also apply to use of Northampton School for Girls provided ICT technologies (e.g. laptops, email, data etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I will always lock or sign out of any device I am not actively using or will be leaving unattended.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, my line manager or appropriate person.
- I will immediately report and potential data breaches to the Head Teacher.
- I will only use equipment that is provided by the school for teaching and school-related activities.
- I understand that if I leave Northampton School for Girls, all my digital accounts will be suspended and my data deleted at the Trust's discretion.

I will be professional in my communications and actions when using Northampton School for Girls **systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the schools GDPR policy guidance on consent for digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- If I am responsible for updating social networking sites on behalf of the school, I will do so in accordance with the school's policies and the site guidance.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities. This includes canvassing, lobbying, advocacy, or personal endorsement that has not been ratified by the school. All information discussed or received of a sensitive or confidential nature will remain so and only discussed with relevant key staff such as the Principal or DSL.

Ensuring safe and secure access to technologies and ensure the smooth running of the online platform (Google):

- When I use my personal digital device (e.g. personal laptop/tablets/phones) at home, I will follow the rules set out in this agreement and need to ensure that I am using the device on a secure network.
- I will not use personal email addresses for school ICT services nor to register for any services on behalf of the school.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes) I will contact the ICT Support team for advice.

- I will ensure that I place my data in my approved areas (my Home Directory/OneDrive area) or a shared area if appropriate and I have been given access. If I house data anywhere else other than these approved locations I understand that the school IT service will not back it up and I will take responsibility for backing up any such data. I will not house any personal data on the school system.
- I will not try to upload, download or access any materials which are illegal (any data covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have been given permission to.
- I will not disable or cause any damage to school/academy equipment, or any equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the schools Data Protection GDPR Policy. Where digital personal data is transferred outside the secure local network, you must take the necessary steps to ensure that the data is shared securely by either encrypting, password protecting or through the use of Google Drive. Paper based protected and restricted data must be held in lockable storage.
- I understand that GDPR law requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not share my personal email address or phone number with students or parents/carers.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions inside and outside of NSG:

- I understand that this Acceptable Use Policy applies not only to my work and use of Northampton School for Girls digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Northampton School for Girls
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action in line with the school's Disciplinary Policy
- I have read and understand the above and agree to use the school digital technology systems for Online Learning and my own devices within these guidelines.

Signed:

Name: Date:

Appendix B – Acceptable use of technology policy for students

We ask all young people and adults to sign an Acceptable Use of Technology Policy, which is a document that outlines who we expect them to behave when they are online and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on the academy site and outside).

We understand the importance of children and young people being able to use the internet for education and personal development. This includes social media platforms, games and apps. We aim to support children and young people in making use of these in our work. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times. Ensuring student safety online is a partnership between the student, their parents/carers and school and all have a role to play in it and need to work together.

This agreement is part of our overarching code of behaviour for children and young people and staff and volunteers. It also fits with our overarching online safety policy. If you would like to know more about this, please speak to the head Teacher or the DSL.

More information about online safety for parents/carers is available from:

- https://www.ceop.police.uk/safety-centre/
- https://www.thinkuknow.co.uk/
- https://educateagainsthate.com/parents/
- https://nationalonlinesafety.com/guides
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting
- https://www.internetmatters.org/
- https://www.net-aware.org.uk/
- https://www.childnet.com/resources/

Websites such as TikTok, Facebook, etc. are 13+ and YouTube is 13+ and 11+ with parent/carer permission. Please find out more about this at https://nationalonlinesafety.com/guides. Please be aware that staff may direct students between the ages of 11 and 13 to YouTube videos for the purposes of learning. These will be age appropriate in content and by signing this agreement you are giving parent/carer permissions for this.

More information about online safety for children and young people is available from:

- https://www.thinkuknow.co.uk/
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/
- https://www.ceop.police.uk/safety-centre

Students: please read the following agreement and discuss it with your parents/carers.

Parents/carers: please read and discuss this agreement with your child and then sign it, then ask your child to sign it. If you have any questions or concerns please speak to [add name/job title].

Young person's agreement

1. I will treat myself and others with respect at all times. When I am online or using any device, I will treat everyone as if I were talking to them face to face.
2. I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access; the language I use and the information I share.
3. I will try to be positive and creative to learn and share, and develop new skills, and to have fun. I will make sure my use of technology does not harm anyone else.
4. I will only access age appropriate websites, social media platforms, games and apps that are for school use.
5. I will not download copyrighted material (e.g. music, text, video etc.).
6. It can be hard to stop using technology sometimes. I will try to use it in moderation and not let it affect other areas of my life (such as sleep).
7. I will consider my online reputation with everything I post and share – I know anything I do can be shared and might stay online forever (even if I delete it).

8. I will not deliberately browse, download or upload material that could be considered offensive or illegal. This includes sites that encourage hate or discrimination. If I accidentally come across any such material I will report it immediately to the school. If I am not in school I will inform my parent/carer.
9. I will not send anyone material that could be considered threatening, bullying, offensive or illegal. Cyber bullying (along with all bullying) will be taken extremely seriously.
10. I will never take secret video, photos or recordings of teachers or students, including during remote learning. 11 I will not give out any personal information online, such as my name, phone number or address.
11. I will not reveal my login, ID's or passwords to anyone and change them regularly. If someone else knows my passwords I will tell a teacher.
12. I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents/carers and am accompanied by a trusted adult.
13. If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to a trusted adult. In school this might be [enter name].
14. I understand that my internet use at Northampton School for Girls will be monitored and logged and can be made available to the school.
15. I will not try to bypass online security in any or access any hacking files or tools. This is a criminal activity.
16. I will only access my own documents and files and not try to view, change or delete other people's files or user areas without their permission.
17. When learning remotely using Google Classroom, teachers and staff will not behave any differently to when we are in school. I will do the same.
18. I will only use personal devices in school if I have permission to do so.
19. I understand that it is illegal to possesses, distribute, show and make indecent images of children, this includes printing and viewing or 'downloading'. I understand that staff can search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

Online Learning (Google classroom)

Northampton School for Girls uses Google classroom as the learning platform providing communication to staff classes and student groups. I agree that:

- I will use Google Classroom and other authorised websites (for example Hegarty maths, Educake, Seneca Learning) to complete learning activities.
- I will ensure that all work uploaded or files sent will be appropriate.
- I will only use the chat function to contact my teacher if I need help with the work set. If this is required I understand that this needs to be appropriate.
- I will limit the use of the chat functionality with other students, and when used will make sure that it is appropriate as records are kept of all chats.
- I will not use the video functionality. If needed, and requested to by a member of staff, I can activate my microphone to talk, but must be appropriate.
- I understand that lessons/video communication may be recorded for safety and for use by my teacher within google classroom.

I understand that these rules are designed to keep me safe and that if I choose not to follow them, school staff may contact my parents/carers.

Signatures:

We have discussed this online safety agreement and agree to follow the rules set out above.

Signature: ……Parent/carer ……Student

Student Name :…… Date: ……