NORTHAMPTON SCHOOL FOR GIRLS

Title:	Online safety and Acceptable Use Policy
Associated Policies:	• Safeguarding and Child Protection • Data Protection • Freedom of Information • Anti-Bullying • Behaviour • Child-on-Child Abuse • Filtering and Monitoring procedures.

1. Statement of Aims

Information and communications technology (ICT) is an integral part of a schools teaching, pastoral and administrative functions and is a critical resource for students, staff, and governors,

However, the misuse and malpractice of ICT resources and facilities also pose significant risks to data protection, online safety and safeguarding.

This policy:

- Sets guidelines and rules on the use of school ICT resources and the use of mobile and smart tech devises for staff, students, parents/carers and governors to secure the safe use of school systems.
- Establishes clear expectations for the way all members of the school community engage with each other online.
- Supports the school's policies on data protection, online safety and safeguarding.
- Supports the school in effectively teaching students to stay safe online. This teaching is underpinned by the 4 key categories of risk.

The 4 key categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, 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

This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary and behaviour policies.

2. Legislation and Guidance

This policy is based on a wide range of legislation and guidance and is underpinned by the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, 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 (as amended), 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 students' electronic devices where they believe there is a 'good reason' to do so.

This policy also refers and complies with legislation and guidance around data and GDPR including:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

3. Roles and Responsibilities

3.1 The governing board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also monitor the staff online safety training provision and filtering and monitoring practice in the school as required and at least annually, to ensure they have the knowledge to ensure effective safeguarding.

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting these standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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 (Appendix C)

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) [and deputy/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 headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT lead to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT lead and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents including of cyber-bullying are recorded and dealt with appropriately in line with school policies.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Ensuring that any online safety incidents including of cyber-bullying are recorded and dealt with appropriately in line with school policies.

This list is not intended to be exhaustive.

3.4 The ICT lead

The ICT lead is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conduct a full security automated check and monitoring the school's ICT systems on a weekly basis.
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency 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 (Appendix C), and ensuring that students follow the school's terms on acceptable use (Appendix A)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety and cyber-bullying incidents are logged and dealt with appropriately in line with this 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.'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix A)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix C)

4. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and students. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

Staff, students, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

4.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. Members of staff or students who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

4.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed and be configured to perform such updates regularly or automatically. Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

To access the internet and school services using their personal devices must complete and sign the schools "Bring you own device policy" This secures our system.

4.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy found on the school website.

4.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the ICT lead. Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT lead immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

4.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as student information) out of school if they have been specifically authorised to do so by the headteacher.

5. Protection from cyber attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure.
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email.
  - Respond to a request for bank details, personal information or login details.
  - Verify requests for payments or changes to information.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents.
- Investigate whether our IT software needs updating or replacing to be more secure.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.
- Put controls in place that are:
  - **Proportionate**: the school will verify this using a third-party audit (such as 360 degree safe) annually to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be.
- Back up critical data occurs automatically and in multiple places online with an air gap and also locally on dedicated back-up servers at 10pm every evening.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Easy PC, patched by the IT technician and supported by the TURN IT ON support contract.
- Make sure staff:
  - Dial into our network using a virtual private network (VPN) when working from home.
  - Multi-factor authentication is initiated on a range of accounts including IT admin.
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights.
- Have a firewall in place that is switched on.
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested by the IT team every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

6. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships and sex education and health education in secondary schools

In **KS3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.
- Students in **KS4** will be taught:
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including imprisonment.
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

7. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website This policy will also be shared with parents/carers.

Regular communication with parents/carers will support them to know:

- What systems the school uses to filter and monitor online use

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- What support and guidance is available to support parents to keep their children safe online.

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

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

8. Cyber Bullying

8.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

8.2 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 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 as part of the wider anti-bullying work with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they 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 school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8.3 Examining electronic devices.

Any searching or confiscation of students will be carried out in line with:

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

According to the behaviour policy the headteacher, and staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will follow the guidance contained in the school safeguarding and child protection policy:

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

8.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

NSG recognises that AI has many uses to help students learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

NSG will treat any use of AI to bully students in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school. (Please see separate A1 policy)

9. Acceptable Use of the Internet in School

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in the appendices.

10. Student using mobile devices in school

Any use of mobile devices in school by students must be in line with our NSG Expects and the schools acceptable use agreement (Appendix A) Students must sign the school "Bring Your Own Device (BYOD) agreement before connecting to our internal Wi-Fi access points.

Any breach of these expectations and the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device and if involves illegal activity or content, or otherwise serious incidents, will be reported to the police.

11. Staff using work devises outside of school

Guidance for members of staff outlining the terms of acceptable use and how staff can ensure their devices and ICT access remain secure can be found in (Appendix B and C)

APPENDIX A: Acceptable use of ICT agreement (Students and Parents)

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 Headteacher 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 your child's Head of Year/Head of Academic Standards.

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.
12) 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.
13) 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.
14) 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, for example my form tutor, Pastoral Officer, Head of Academic Standards.
15) I understand that my internet use at Northampton School for Girls will be monitored and logged and can be made available to the school and other safeguarding organisations as necessary including the police.
16) I will not try to bypass online security in any or access any hacking files or tools. This is a criminal activity.
17) 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.
18) 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.
19) I will follow the NSG Expects and the Code of Conduct which clearly explain the expectations about using mobile phone and other mobile devices in school. I understand the consequences for not following these rules.
20) 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.
21) | will not use AI technology to create false images or media, to imitate my own work.

22) I understand that when I am non longer on role at NSG my email access and all related files access will be removed within 3 months at the latest.

<u>Online Learning (Google classroom)</u>

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 Dr Frost, Edu cake, 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.

Signatures: …………………………………… (Parent/carer) ……………………………………………. (Student)

Student Name :………………………………… Student Form ………………… Date: ………………….

APPENDIX B: Staff guidance on their use of school-based ICT facilities, resources and equipment

Access to school ICT

The school's ICT lead manages access to the ICT facilities, resources and equipment for all school staff. Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities, resources and equipment. Any member of staff who has access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT lead/ITC technical team.

Use of phones and email

The school provides each member of staff with an email address. This email account should be used for work purposes, and all work-related business should be conducted using the email address the school has provided. Staff must not share their personal email addresses with parents/carers and students and must not send any work-related materials using their personal email account.

Staff must take care with the content 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. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. If staff send an email in error that contains the personal information of another person, ie a student, they must inform the DSL immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or students.

Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time.
- Does not constitute a breach of the acceptable use agreement.
- Takes place when no students are present.
- Does not interfere with their jobs or prevent other staff or students from using the facilities for work or educational purposes.

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos). Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities and any subsequent subject access request. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's acceptable use agreement. Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parents/carers could see them. Staff should take care to follow the school's training and guidance on use of social media and use of email to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is always appropriate. For further guidance on this staff should contact the ICT lead.

Remote access

We allow staff to access the school's ICT facilities and materials remotely by 2 means:

1) Via cloud storage facility such as One Drive and Google Drive. All files are automatically backed up.

2) Access SIMS is via our Virtual Private Network (VPN). Our VPN is managed by the school and provided by Securely

All Security arrangements including Protocols for remote access and staff request remote access are managed by the ITC technical team overseen by the ICT lead.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the ICT lead may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy which can be found on the school web site.

School social media accounts

The school has official Facebook Twitter and Instagram accounts, managed by an identified team 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.

Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school filters and monitors the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited.
- Key words typed.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.
- Any other electronic communications.

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school use SENSO to manage devices and monitor keywords entered. Securely filters site access and reports on this access. Both programmes access this in a hierarchical risk manner which is determined in part by the school.

The school filters and monitors ICT use in order to:

- Safeguard students in line with the expectations laid out in Keep Children Safe In Education.

Filtering and monitoring also supports the school to:

- Obtain information related to school business.
- Investigate compliance with school policies, procedures and standards.
- Ensure effective school and ICT operation.
- Conduct training or quality control exercises
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

The governing board is responsible for making sure that:

- Staff are aware of the DfE's filtering and monitoring standards and the schools filtering and monitoring systems.
- Staff are receive appropriate training on these systems related to their roles and responsibilities. For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns.
- Staff are aware that they will regularly review the effectiveness of the school's monitoring and filtering systems.

The school's designated safeguarding lead (DSL) is responsible for monitoring and managing the filtering and monitoring systems and processes that are in place.

All staff members are responsible for:

- Ensuring they do not use the device in any way that would violate the school's filtering and monitoring systems.
- Reporting any concerns over the security of their device to the ICT lead and the DSL.
- Attending all training as directed to ensure they are aware of their safeguarding responsibilities.
- Inform the ICT lead and technical team where their curriculum might be affected by the filtering setting in a detrimental way.

Training should ensure staff:

- Understand their responsibilities around filtering and monitoring.
- Understand their responsibility around developing the ability of students to recognise dangers and weigh up risks in online activity developing the resilience to ensure they make healthy long-term choices and keep them safe from harm in the short term.
- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Support the "appropriate "level of filtering as to not affect the effective delivery of the PSHE and other curriculums

APPENDIX C: Acceptable use of ICT agreement (Staff, Governors and volunteers)

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:

1) I understand and accept that Northampton School for Girls will fully monitor my use of the school digital technology and communications systems.
2) I understand that if my activity causes any concerns, safeguarding software installed by the school may automatically alert appropriate safeguarding specialists who may choose to investigate depending on the content of the alert.

3) 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.
4) I will always lock or sign out of any device I am not actively using or will be leaving unattended.
5) I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, my line manager or appropriate person.
6) I will immediately report and potential data breaches to the Head Teacher.
7) I understand that if I leave Northampton School for Girls, all my digital accounts will be suspended, and my data deleted at the school's discretion.
8) I will be professional in my communications and actions when using Northampton School for Girls systems:
9) I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
10) I will communicate with others in a professional manner, I will not use aggressive or inappropriate language.
11) 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.
12) 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.
13) I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
14) 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 Headteacher or DSL.

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

15) 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
16) I will not use personal email addresses for school IT services nor to register for any services on behalf of the school.
17) 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 IT Support team for advice.
18) I will ensure that I place my data in my approved areas (my Home Directory/OneDrive /Google Drive area) or a shared area if appropriate thatI 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.
19) 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.

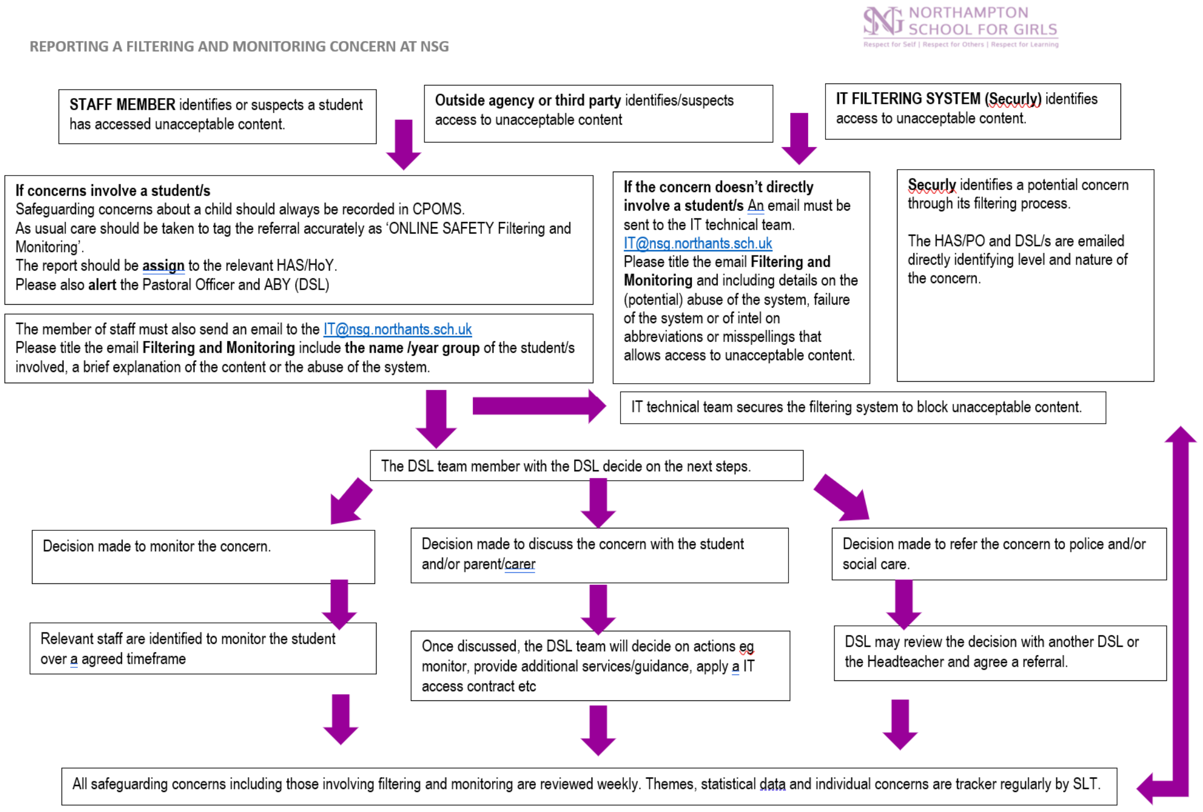
20) I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have been given permission to.
21) I will not disable or cause any damage to school/academy equipment, or any equipment belonging to others.
22) 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/encrypted storage.
23) 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.
24) I will immediately report any damage or faults involving equipment or software; however this may have happened.
25) I will not share my personal email address or phone number with students or parents/carers.
26) When using the internet in my professional capacity or for school sanctioned personal use:
27) I will ensure that I have permission to use the original work of others in my own work.
28) Where work is protected by copyright, I will not download or distribute copies (including music and videos).
29) | will not use AI technology to create false images or media, to imitate my own work.

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 D: Filtering and Monitoring referrals flow diagram



REPORTING A FILTERING AND MONITORING CONCERN AT NSG

STAFF MEMBER identifies or suspects a student has accessed unacceptable content.

Outside agency or third party identifies/suspects access to unacceptable content

IT FILTERING SYSTEM (Securly) identifies access to unacceptable content.

If concerns involve a student/s
Safeguarding concerns about a child should always be recorded in CPOMS.
As usual care should be taken to tag the referral accurately as 'ONLINE SAFETY Filtering and Monitoring'.
The report should be **assign** to the relevant HAS/HoY.
Please also **alert** the Pastoral Officer and ABY (DSL)

The member of staff must also send an email to the IT@nsg.northants.sch.uk
Please title the email **Filtering and Monitoring** include **the name /year group** of the student/s involved, a brief explanation of the content or the abuse of the system.

If the concern doesn't directly involve a student/s An email must be sent to the IT technical team. IT@nsg.northants.sch.uk
Please title the email **Filtering and Monitoring** and including details on the (potential) abuse of the system, failure of the system or of intel on abbreviations or misspellings that allows access to unacceptable content.

Securly identifies a potential concern through its filtering process.

The HAS/PO and DSL/s are emailed directly identifying level and nature of the concern.

IT technical team secures the filtering system to block unacceptable content.

The DSL team member with the DSL decide on the next steps.

Decision made to monitor the concern.

Relevant staff are identified to monitor the student over a agreed timeframe

Decision made to discuss the concern with the student and/or parent/carer

Once discussed, the DSL team will decide on actions eg monitor, provide additional services/guidance, apply a IT access contract etc

Decision made to refer the concern to police and/or social care.

DSL may review the decision with another DSL or the Headteacher and agree a referral.

All safeguarding concerns including those involving filtering and monitoring are reviewed weekly. Themes, statistical data and individual concerns are tracker regularly by SLT.