NORTHAMPTON SCHOOL FOR GIRLS
Respect for Self | Respect for Others | Respect for Learning

Online Safety and Acceptable Use Policy

Author:	AFY
Approval Date:	22 September 2025
Approval Body:	Full Governing Board
Review Date:	September 2026
Version:	V2

Version	Date	Updates
V2	**September 2025**	Formatting changes and changes to staff agreement, all highlighted in yellow.

Associated Policies	• Safeguarding and Child Protection • Data Protection • Freedom of Information • Anti-Bullying • Behaviour • Child-on-Child Abuse • Filtering and Monitoring procedures • Use of Artificial Intelligence (AI)

1. Executive Summary

1.1 This policy outlines Northampton School for Girls' commitment to maintaining a safe, respectful, and secure digital environment. It provides clear guidelines for the appropriate use of technology by staff, students, governors, volunteers, contractors, and visitors. Our policy is aligned with statutory safeguarding guidance and relevant legislation. Key focuses include:

- Promoting safe and respectful online behaviour.
- Protecting personal and school data.
- Managing cybersecurity risks including mandatory use of Multi-Factor Authentication (MFA/2FA).
- Prohibiting the use of unauthorised external storage devices (USB drives).
- Providing regular and responsive online safety education.
- Ensuring continuous professional development, including identifying and addressing gaps in staff knowledge (e.g., phishing awareness).
- Adopting a zero-tolerance approach to cyberbullying and inappropriate use of AI.

All users are expected to comply fully, with breaches addressed through disciplinary procedures.

2. Statement of Aims

2.1 IT is an integral part of teaching, pastoral care, and administration. However, misuse poses significant risks to safeguarding and data protection. This policy will:

- Set guidelines for the safe use of school IT resources.
- Establish clear expectations for online engagement.
- Support safeguarding and data protection.
- Teach students to stay safe online through the four key categories of risk: Content, Contact, Conduct, and Commerce.

This policy applies to all users: staff, students, governors, volunteers, contractors, and visitors.

3. Legislation and Guidance

3.1 This policy reflects statutory and non-statutory guidance including:

- Keeping Children Safe in Education (DfE)
- Teaching Online Safety in Schools (DfE)
- Preventing and Tackling Bullying (DfE)
- Searching, Screening, and Confiscation (DfE)
- Relationships and Sex Education (DfE)
- Meeting digital and technology standards in schools and colleges (DfE)

Relevant legislation includes:

- Education Acts 1996 & 2011
- Equality Act 2010
- Data Protection Act 2018 and UK GDPR
- Computer Misuse Act 1990
- Telecommunications (Lawful Business Practice) Regulations 2000

4. Roles and Responsibilities

4.1 **The Governing Board will:**

- Monitor and hold the Headteacher to account for implementation.
- Ensure staff online safety training occurs annually and address identified gaps in knowledge.
- Review filtering and monitoring systems annually.
- Ensure teaching adapts to meet the needs of vulnerable children.

4.2 **The Headteacher will:**

- Ensure consistent policy implementation and staff understanding.
- Facilitate additional training where skills gaps are identified (e.g., phishing awareness).

4.3 **The designated safeguarding lead (DSL) will:**

- Lead responsibility for online safety.
- Review filtering and monitoring processes.
- Report periodically to the Governing Board to ensure oversight.
- Conduct annual risk assessments.

4.4 **The Network Officer will:**

- Manage and maintain filtering, monitoring, and security.
- Conduct weekly system checks.
- Enforce strong password policies across all systems, ensuring regular updates and compliance with cybersecurity best practices.

4.5 **All staff and volunteers will:**

- Follow acceptable use policies.
- Report any concerns to the DSL.
- Support online safety education.
- Engage in cybersecurity and online safety training, particularly where gaps in skills are identified.
- Use Two-Factor Authentication (2FA) when connecting to school-provided services such as email accounts and cloud storage platforms.

4.6 **Parents and carers will:**

- Support the school's online safety approach
- Ensure their child reads and understands acceptable use agreements.

4.7 **Visitors will:**

- Follow the school's IT policies where relevant.

5. Data security

5.1 All users will take the following steps to ensure robust data security on all systems:

- Use strong passwords (password complexity is enforced); periodic updates, and account security.
- Keep software, firewalls, antivirus, and security features up to date; systems will be periodically reviewed to address evolving cyber threats.
- Follow the school’s BYOD policy when using personal devices; authorisation from the Headteacher is required to access or transport school data on personal devices or USBs.
- Store all personal data securely, in line with GDPR and the school’s Data Protection Policy
- Use encryption where appropriate to protect sensitive information.

- Log out of systems, lock devices when unattended, and shut down at the end of each day to prevent unauthorised access.
- Not attempt to access systems or files without permission, all access rights are assigned and reviewed by the Network Officer. Any accidental access or misdirected information must be reported immediately to the IT team
- Not download, store, or transport student or staff data on unauthorised external storage devices.

6. Cybersecurity

6.1 NSG will undertake the following steps to ensure robust, continuous and up to date cybersecurity measures are in place for all users:

- Provide regular staff training, including phishing identification, email safety, and cybersecurity awareness. Training will cover how to check email sender addresses, verify requests for bank details or payment changes, and respond to suspicious messages. This training will also be included in staff induction.
- Ensure staff are aware of how to report cybersecurity incidents, including whom to contact (e.g., DSL, Network Officer, Data Protection Officer) and the required procedures.
- Require the mandatory use of VPN and Multi-Factor Authentication (MFA/2FA) for remote access, critical system access, and school-provided services including email and cloud storage.
- Prohibit the use of unauthorised external storage devices (e.g., USB drives) and personal cloud storage platforms for school data.
- Conduct third-party cybersecurity audits (e.g., 360 Safe) annually to test the effectiveness of controls.
- Maintain a layered approach to cybersecurity:
    - Ensure all systems are kept up to date, with software updates and security patches applied promptly.
    - Maintain an active and enabled firewall.
    - Conduct regular access and permissions reviews to ensure staff have the appropriate level of access.
- Automatically back up critical data daily, including online backups with an air gap and local backups to dedicated backup servers (e.g., at 10 p.m. each evening).
- Delegate responsibility for management information system (MIS) security to Easy PC, supported by the IT technician and the Turn It On support contract.
- Assess the security of suppliers and contractors, including verification of Cyber Essentials certification where appropriate.
- Develop, review, and test the incident response plan with the IT team every six months or after any significant incident, using the NCSC's 'Exercise in a Box' tool to simulate and improve real-world response readiness.
- Never engage with ransom requests in the event of a ransomware attack, as this does not guarantee recovery of data.

7. Educating students

7.1 Through the curriculum, students will:

- Learn to stay safe, respectful, and responsible online.
- Understand harmful content, cyberbullying, harassment, and online abuse.
- Protect their online identity and privacy, and understand the permanence of online behaviour.
- Recognise inappropriate content, contact, and conduct, and know how to report concerns.
- Understand the impact of viewing harmful or explicit content and that sharing/viewing indecent images (including of children) is illegal.

- Learn how consent works in all contexts, including sexual consent, and how to recognise or withdraw consent.
- Develop data literacy, understanding how information is generated, collected, shared, and used online.

  Know their rights, responsibilities, and opportunities online, including the same expectations of behaviour online and offline.
- Learn where to get help and how to report or manage issues online.

Teaching will align with statutory Relationships and Sex Education (RSE) and Health Education requirements, including how technology affects safety, privacy, and wellbeing.

Where necessary, content will be adapted for vulnerable students, victims of abuse, and students with SEND.

8. Educating parents/carers

8.1 The school will raise parents' and carers' awareness of online safety through regular communication, including letters, newsletters, meetings, and the school website.

Parents/carers will be informed about:

- The school's filtering and monitoring systems.
- The online activities, platforms, and tools students are asked to use, including who from school may interact with them online.
- Where to find additional guidance and support, including resources from organisations such as CEOP, NSPCC, National Online Safety, and Childnet.
- How to access and review the school's Online Safety and Acceptable Use Policies.

If parents/carers have any concerns or questions about online safety, they are encouraged to contact the headteacher or Designated Safeguarding Lead (DSL). Concerns about this policy can also be raised with any member of staff.

The school aims to work in partnership with parents and carers to promote a consistent message about staying safe online, both at school and at home.

9. Cyber Bullying

9.1 **Definition**

Cyberbullying is the repetitive, intentional harming of one person or group by another, using online platforms such as social media, messaging apps, or gaming sites, where there is an imbalance of power. It is addressed as part of our anti-bullying and behaviour policies.

9.2 **Prevention and Education**

Students will be taught what cyberbullying is, why it happens, and how to report it, including as a bystander. Cyberbullying will be discussed through PSHE, tutor time, and across the curriculum where appropriate.

Staff, governors, and volunteers will receive training on recognising, preventing, and responding to cyberbullying as part of safeguarding training.

Parents/carers will be provided with guidance on recognising the signs of cyberbullying, how to report it, and how to support their child.

9.3 **Response to Incidents**

All incidents will be managed according to the behaviour policy. Where illegal, harmful, or inappropriate material has been shared, the school will act swiftly to contain the incident.

The Designated Safeguarding Lead (DSL) will liaise with police and external services where appropriate.

9.4 **Examining electronic devices.**

Searches and confiscations will follow DfE guidance on searching, screening, and confiscation and UKCIS guidance on sharing nudes/semi-nudes. Authorised staff may search devices if they have reasonable grounds to suspect a risk to staff/students, a banned item, or evidence of an offence.

Complaints about searches will follow the school complaints procedure.

9.5 **Artificial intelligence (AI)**

Use of AI tools, such as deepfakes, to bully or harm others will be treated as a serious bullying incident.

Staff will carry out risk assessments when introducing new AI tools in school. (See the school AI policy.)

10. Acceptable Use of the Internet

10.1 All students, parents/carers, staff, volunteers, governors, and visitors (where relevant) are required to follow the school's acceptable use expectations.

All users must:

- Sign an acceptable use agreement before accessing school systems.
- Use internet access for educational or work-related purposes only, or to fulfil the duties of their role.
- Comply with the school's monitoring and filtering systems. The school monitors the websites visited by students, staff, volunteers, governors, and visitors (where applicable) to ensure appropriate use, and restricts access through filtering systems where needed.

11. Mobile Devices

11.1 Any use of mobile devices in school by students must comply with the NSG Respects, the Acceptable Use Agreement (Appendix A), and the school's Bring Your Own Device (BYOD) policy.

Students must sign the BYOD agreement before connecting their personal devices to the school's internal Wi-Fi access points.

Any breach of these expectations or agreements may trigger disciplinary action in line with the school behaviour policy, including the possible confiscation of the device.

Incidents involving illegal activity, illegal content, or other serious breaches will be reported to the police and dealt with under any appropriate internal safeguarding procedures

12. Staff using work devices and systems outside of school

12.1 If staff are required to use their work devices and systems outside of school, they must do the following:

- Adhere to remote access protocols, including VPN and MFA.
- Secure handling of data is mandatory.
- Student or staff data must not be stored or transferred using unauthorised devices.

13. VPN Access and Remote Working

13.1 This section applies only to staff members who are authorised to access the school's Virtual Private Network (VPN) for remote working.

Authorised users must:

- Use the VPN solely for school-related work. Personal use while connected to the VPN is prohibited.

- Only use school-authorised and configured devices to access the VPN.
- Protect their VPN credentials and Two-Factor Authentication (2FA) keys. Credentials must not be shared.
- Complete mandatory cybersecurity awareness training before receiving VPN access and participate in refresher training when required.
- Ensure that devices accessing the VPN have up-to-date antivirus software, operating system patches, and automatic updates enabled.
- Lock devices when unattended and secure them with strong passwords or biometric authentication.
- Avoid using public or unsecured Wi-Fi networks when connecting to the VPN.
- Follow the school’s Data Protection Policy. Sensitive data must not be downloaded or stored on personal devices; remote access should be limited to viewing and interacting with data.
- Report any cybersecurity incidents (e.g., phishing attempts, suspicious activity) immediately to the IT department.

The school’s IT department will monitor VPN use for security purposes. Logs will be reviewed periodically to ensure compliance. Misuse may result in suspension of VPN access and disciplinary action.

APPENDIX A: Student Acceptable Use Agreement

We ask all students 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 recognise the educational value of the internet and digital tools and aim to support safe, positive use. Safeguards must be in place to ensure that children and young people are kept safe at all times.

Ensuring student safety online is a shared responsibility between students, parents and carers and school staff.

The below agreement is part of our overarching code of behaviour and online safety policy.

Additional advice for parents and carers can be found at:

- 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/

Student Agreement

Online Behaviour

I will treat myself and others with respect at all times, online and offline.

I will be responsible for my behaviour when using the internet, including the resources I access, the language I use, and the information I share.

I will act positively and creatively, developing skills and having fun without causing harm to others.

I will only access age-appropriate websites, social media platforms, games, and apps intended for my use.

I will not download copyrighted material (e.g., music, videos) without permission.

I will use technology in moderation and ensure it does not negatively affect my wellbeing (e.g., sleep).

I will consider my online reputation with everything I post or share, understanding that content may remain online permanently.

Safety and Security

I will not deliberately browse, download, or upload material that could be considered offensive or illegal.

If I encounter such material accidentally, I will report it to a trusted adult (such as my form tutor, Pastoral Officer, or DSL).

I will not send material that could be considered threatening, bullying, offensive, or illegal.

I will never secretly record, photograph, or film staff or students without permission.

I will not give out personal information such as my full name, phone number, address, or school details online.

I will create strong passwords (using a mix of letters, numbers, and symbols), keep them secret, and change them regularly.

I will not arrange face-to-face meetings with people I meet online unless I have parental permission and am accompanied by a trusted adult.

	I understand that my internet use at Northampton School for Girls will be monitored and logged for safety purposes. I will not attempt to bypass security measures or access hacking tools. I will not access, modify, or delete other people's files without permission. I will report any concerns about online safety or cyberbullying immediately to a trusted adult at school. I will not use personal mobile data networks to bypass school filtering and monitoring. I will treat other people's personal information carefully and will not share it without permission.
Use of Technology and AI	
	I will not use AI technology to create false media, imitate others, or complete work dishonestly. I will only use mobile devices in line with the NSG Expects and Code of Conduct, understanding that breaches have consequences. I understand that recording or screenshotting online lessons (e.g., on Google Classroom) is prohibited unless specifically instructed by a teacher.
Online Learning (Google Classroom and Approved Platforms)	
	I will use Google Classroom and other approved platforms (e.g., Dr Frost, Seneca Learning) responsibly to complete learning activities. I will use the chat function only when necessary to ask my teacher for help and will communicate appropriately. I understand that chats are recorded and monitored. I will not activate video functions unless specifically requested by staff. I understand that lessons may be recorded for safety and review purposes.
Leaving School	
	I understand that when I am no longer on roll at NSG, my email account and access to school systems will be removed within 3 months.
Acknowledgement	
	Student Name: ________________________________ **Student Signature:**_____________________________ **Parent/Carer Name:** ____________________________ **Parent/Carer Signature:** _________________________ **Date:** ____________________

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

Access to School IT

The Network Officer manages access to school IT facilities, resources, and equipment for all staff. Staff will be provided with unique login credentials and passwords, which they must use to access school IT systems. Staff who encounter unauthorised access or require permission changes must contact the Network Officer or IT technical team.

Use of Phones and Email

Staff are provided with a school email address for work purposes only; all professional communication must use this address. Personal email addresses must not be shared with parents/carers or students, nor used to conduct school business.

Email content must be professional and respectful to avoid legal or reputational risk. Emails are subject to legal disclosure under the UK GDPR and Data Protection Act 2018. Deleting an email from an inbox does not mean it cannot be recovered.

Sensitive or confidential attachments must be encrypted. Accidental email errors must be reported to the DSL, following the school’s data breach procedure.

Personal phone numbers must not be shared with parents/carers or students.

Personal Use

- Occasional personal use of school IT is permitted if it:
    - Does not occur during contact time.
    - Adheres to the Acceptable Use Agreement.
    - Does not involve students.
    - Does not interfere with work or others' access.
- Personal files (music, videos, photos) must not be stored on school systems.
- Personal use is monitored and may be subject to a subject access request.
- Personal device use is allowed under the Acceptable Use Agreement; staff should avoid posting personal details that could compromise their professional role.

Social Media

- Staff should ensure all social media use is appropriate.
- For guidance, staff should contact the Network Officer.

Remote Access

- Remote access is provided via:
    - Cloud services (OneDrive, Google Drive) with automatic backups.
    - SIMS access via the school VPN, managed by the IT team.
- Staff must follow all on-site IT rules when accessing systems remotely.
- Devices used remotely must:
    - Be updated with antivirus and system patches.
    - Use Two-Factor Authentication (2FA) for email, cloud, and VPN access.
    - Be locked when unattended.
    - Avoid public or unsecured Wi-Fi connections.
- Confidential and personal data must be handled per the school’s Data Protection Policy.

Use of Two-Factor Authentication (2FA)

- Staff must use 2FA when accessing email, cloud platforms, and the VPN.
- Lost or compromised 2FA tokens or authenticator apps must be reported immediately to the IT team.

Use of AI Tools

- Staff must not use AI to generate official communications, student feedback, reports, or grades without approval.
- AI use for teaching support must follow school guidelines and must not replace professional judgement.

Device and Physical Security

- Devices must be locked or signed out when unattended.
- School devices used offsite must be stored securely.
- Passwords must be strong (including letters, numbers, and symbols), changed regularly, and never shared.

School Social Media Accounts

Only authorised staff may manage or post on official school accounts (Facebook, Twitter, Instagram).

Monitoring and Filtering

- The school uses SENSO and Securely to monitor internet activity, including sites visited, keywords typed, bandwidth, email accounts, telephone calls, and user logs.
- Filtering and monitoring help safeguard students, investigate policy compliance, ensure IT effectiveness, conduct training, prevent crime, and meet legal obligations.
- Only authorised IT personnel may inspect or disclose monitored data.

Staff Responsibilities for Filtering and Monitoring

- Staff must not bypass or interfere with filtering and monitoring systems.
- Concerns about device security must be reported to the Network Officer or DSL.
- Staff must complete all required safeguarding and online safety training.
- Staff should alert the IT team if curriculum delivery is negatively affected by filtering settings.

Data Protection and Breach Reporting

Staff must follow the school's Data Protection and GDPR Policies.

Any suspected data breaches (including misdirected emails or lost devices) must be reported immediately to the DSL and Data Protection Officer.

APPENDIX C: Staff Acceptable Use Agreement

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.

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 investigate.
3. I understand that the rules set out in this agreement also apply to use of Northampton School for Girls provided IT 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 to my line manager or appropriate person.
6. I will immediately report any potential data breaches to the Headteacher.
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, using appropriate language.
11. I will ensure that when I take and/or publish images of others, I do so with their permission and in accordance with the school's GDPR policy guidance on consent.
12. If responsible for updating social networking sites on behalf of the school, I will do so in accordance with the school's policies and site guidance.
13. I will only communicate with students and parents/carers using official school systems.
14. I will not engage in any online activity that may compromise my professional responsibilities.
15. When using my personal digital device (e.g., personal laptop, tablet, phone) at home for work purposes, I will use 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 or attachments in emails unless the source is known and trusted.
18. I will ensure that I place data only in approved locations (Home Directory, OneDrive, Google Drive). I understand that the school IT service will not back up data stored elsewhere.
19. I will not upload, download, or access illegal or inappropriate material and will not attempt to bypass filtering/security systems.

20. I will not install or attempt to install any software or programs without permission.

21. I will not disable or damage school/academy equipment or any equipment belonging to others.

22. I will handle all personal information in line with the school's GDPR Policy.

23. I understand that GDPR law requires me to keep private and confidential any staff or student data to which I have access.

24. I will immediately report any damage or faults involving equipment or software.

25. I will not share my personal email address or phone number with students or parents/carers.

26. When using the internet professionally or for sanctioned personal use, I will respect copyright law.

27. I will ensure I have permission to use the original work of others and will not distribute copyrighted work illegally.

28. I will not use AI technology to create false images or media, or to imitate my own work.

Use of Two-Factor Authentication (2FA)

29. I understand that I must use Two-Factor Authentication (2FA) when accessing school-provided services, including email accounts, cloud storage (e.g., OneDrive, Google Drive), and other designated systems.
30. I will ensure that my authentication devices (such as security keys or authenticator apps) are secured appropriately and report any loss or issues immediately to the IT Department.

VPN Access and Usage

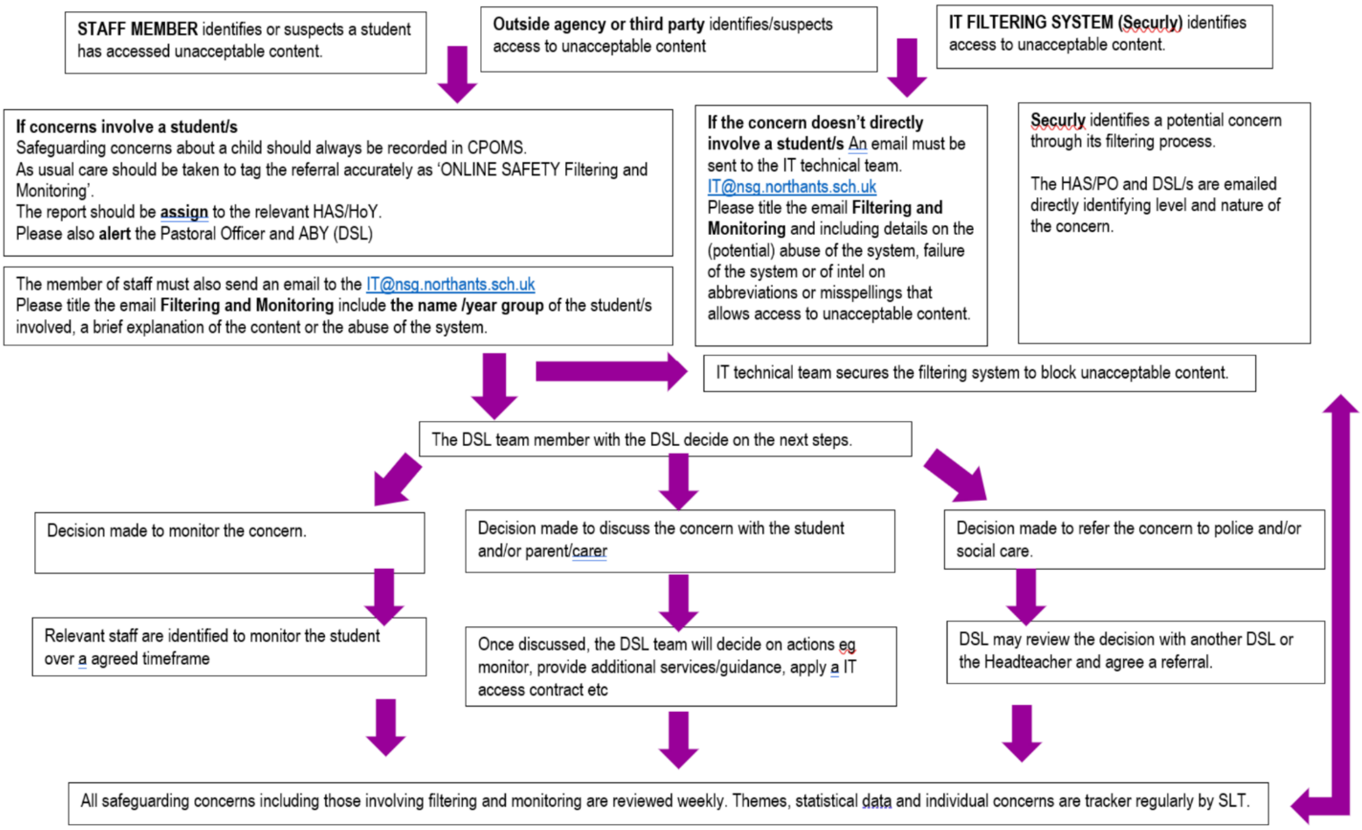
(For authorised users only)

1. VPN access is provided solely for school-related activities.
2. Only school-authorised and configured devices may be used for VPN access.
3. VPN access credentials and 2FA security keys must not be shared.
4. Public or unsecured Wi-Fi must not be used when connecting to the VPN.
5. Devices used for VPN access must be updated with the latest antivirus software and security patches.
6. Any cybersecurity incidents (e.g., phishing attempts, suspicious activity) must be reported immediately to the IT department.

Misuse of the VPN or non-compliance with cybersecurity measures may result in disciplinary action.

Signed: ……………………………………………………. Name: ………………………………… Date: ……………………….

Appendix D: Filtering and Monitoring referrals flow diagram



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.

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

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

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

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

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.